华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform),* 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。**您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。**（http://support.huawei.com/ecommunity/bbs/list_2247.html）



CSBN-HCNA-Security

上机指导书

（学员用书）

ISSUE 2.00



1 手册说明

本手册用于指导学员学习华为安全产品的配置和部署技术，学员可以通过教材的实验说明，掌握本手册中的实验内容。

1.1 适用范围

适用于华为系统安全工程师培训安全课程中涉及的实验内容。

适用防火墙系列包括：

- USG2200&5100 V300R001

1.2 防火墙产品描述

1.2.1 USG2200 产品描述

- 机箱尺寸

USG2200 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

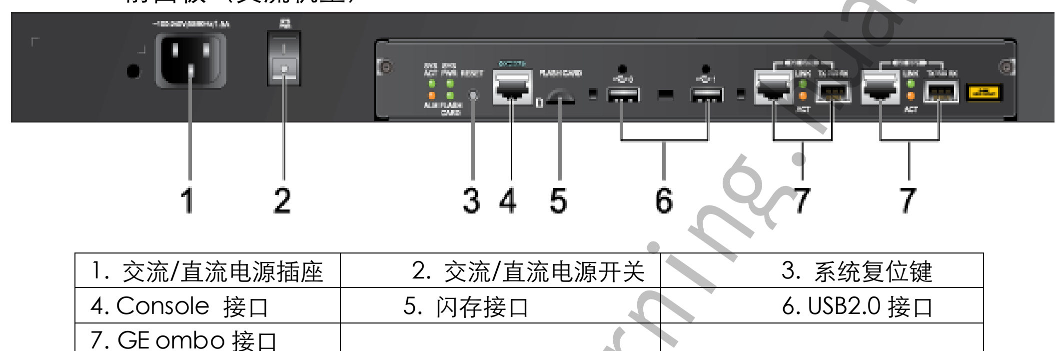
- 前面板

USG2200 的电源和风扇采用内置式，因此从外观上看不到电源和风扇。USG2200 包括 USG2210、USG2220、USG2230、USG2250 四种型号。这四种型号都支持交流机型，其中 USG2250 还有支持直流电源的机型。如下图所示。

USG2200 前面板（直流机型）



USG2200 前面板（交流机型）

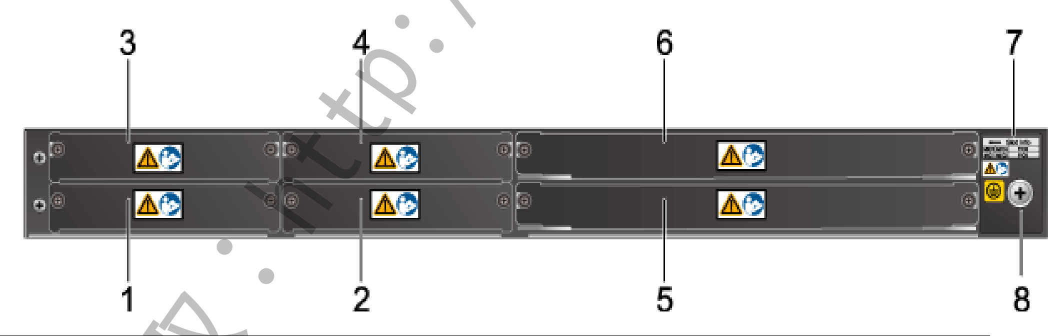


1. 交流/直流电源插座	2. 交流/直流电源开关	3. 系统复位键
4. Console 接口	5. 闪存接口	6. USB2.0 接口
7. GE ombo 接口		

- 后面板

USG2210、USG2220、USG2230、USG2250 后面板布局相同，如下图所示，左侧和中间是 4 个 MIC 插槽，右侧为 2 个 FIC 插槽。

USG2200 后面板



1. MIC1/DMIC1 插槽	2. MIC2/DMIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6 插槽
7.槽位标识	8. 接地端子	

- 槽位分布和排列顺序

FIC5 可插入一个 DFIC 接口卡。如下图所示。

USG2200 槽位编号及排列顺序示意图

MIC3	MIC4	FIC6
MIC1	MIC2	FIC5

提示：MIC1 和 MIC3 两个槽位可以插入两个 MIC 接口卡或插入一个 DMIC 接口卡；

MIC2 和 MIC4 两个槽位可以插入两个 MIC 接口卡或插入一个 DMIC 接口卡；

1.2.2 USG5120 产品描述

- 机箱尺寸

USG5120 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×86.1mm（宽×深×高），可以安装在 19 英寸标准机柜中。

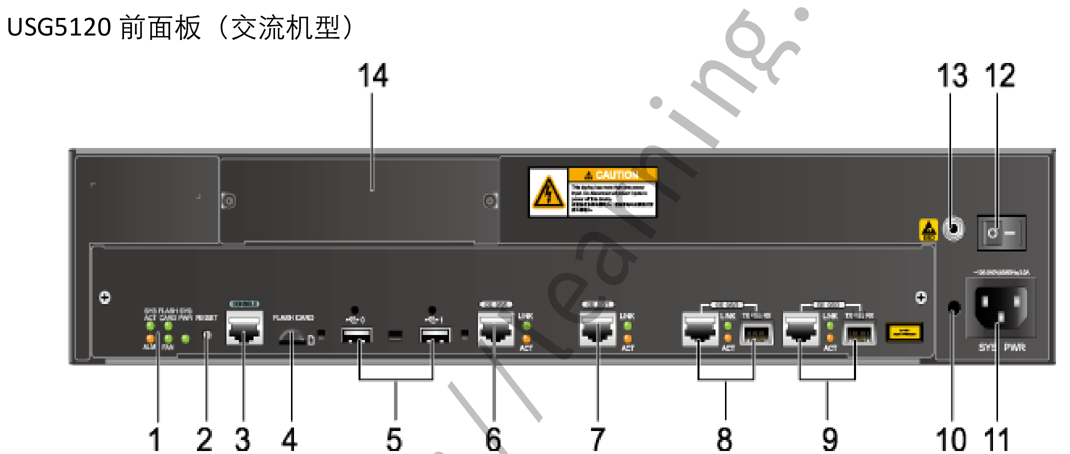
- 前面板

USG5120 有交流和直流两种机型。USG5120 的前面板如下图所示。

USG5120 前面板（直流机型）

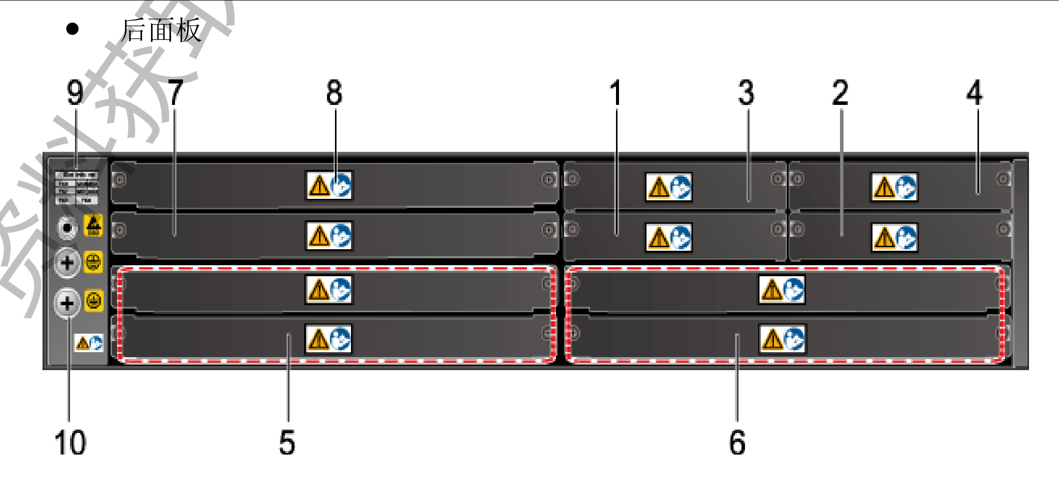


USG5120 前面板（交流机型）



1.指示灯	2.系统复位键	3. Console 接口
4.闪存接口	5. USB2.0 接口	6. 10/100/1000M 以太网接口
7. 10/100/1000M 以太网品	8. GE Combo 接口 2	9. GE Combo 接口 3
10. 卡扣插孔	11. 交流/直流电源插座	12. 交流/直流电源开关
13. 防静电手腕带插孔	14. 防尘面板	

- 后面板



1. MIC1/DMIC1 插　　2. MIC2/DMIC2 插槽　　3. MIC3 插槽
4. MIC4 插槽　　5. FIC5/DFIC5 插槽　　6. FIC6/DFIC6 插槽
7. FIC7 插槽　　8. FIC8 插槽　　9. 槽位标识
10.接地端子

- 槽位分布和排列顺序

USG5120 的 FIC5 和 FIC6 槽位除了可插入一个 DFIC 接口卡外，还可只在下半部分插入一个 FIC 接口卡。此时，为了防尘需要在 DFIC 槽位的上半部分安装一个假面板，以封闭后面板。FIC7 可插入一个 DFIC 接口卡。如下图所示。

USG5120 槽位编号及排列顺序示意图

FIC8	MIC3	MIC4
FIC7	MIC1	MIC2
FIC5	FIC6	

1.2.3 USG5150 产品描述

- 机箱尺寸

USG5150 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×130.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

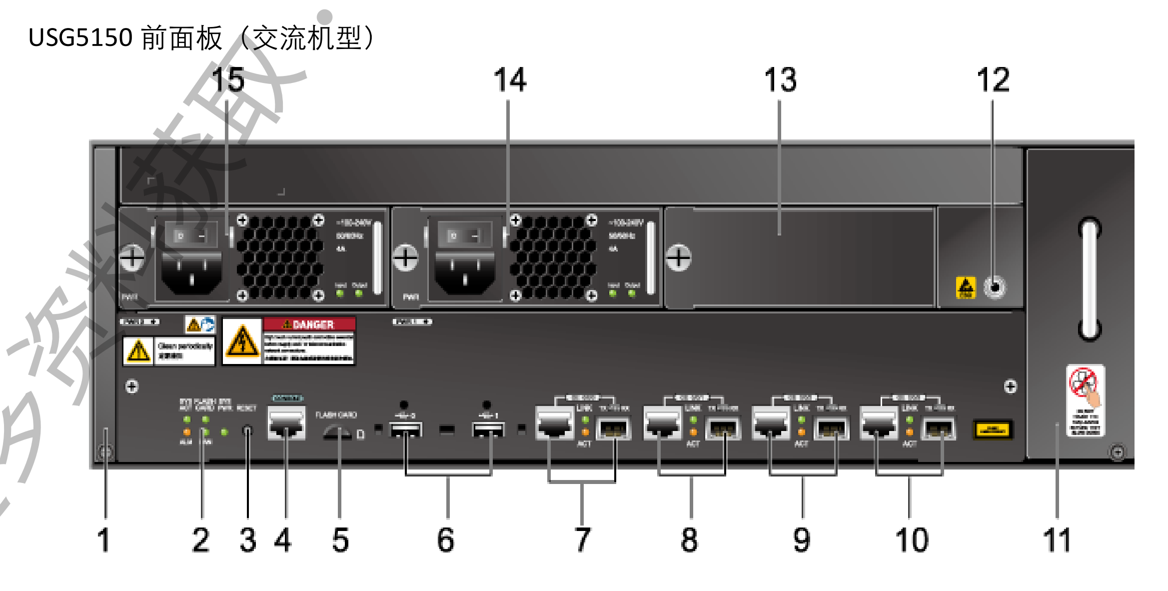
- 前面板

USG5150 的电源和风扇模块均可热插拔，其前面板如下图所示。

USG5150 前面板（直流机型）

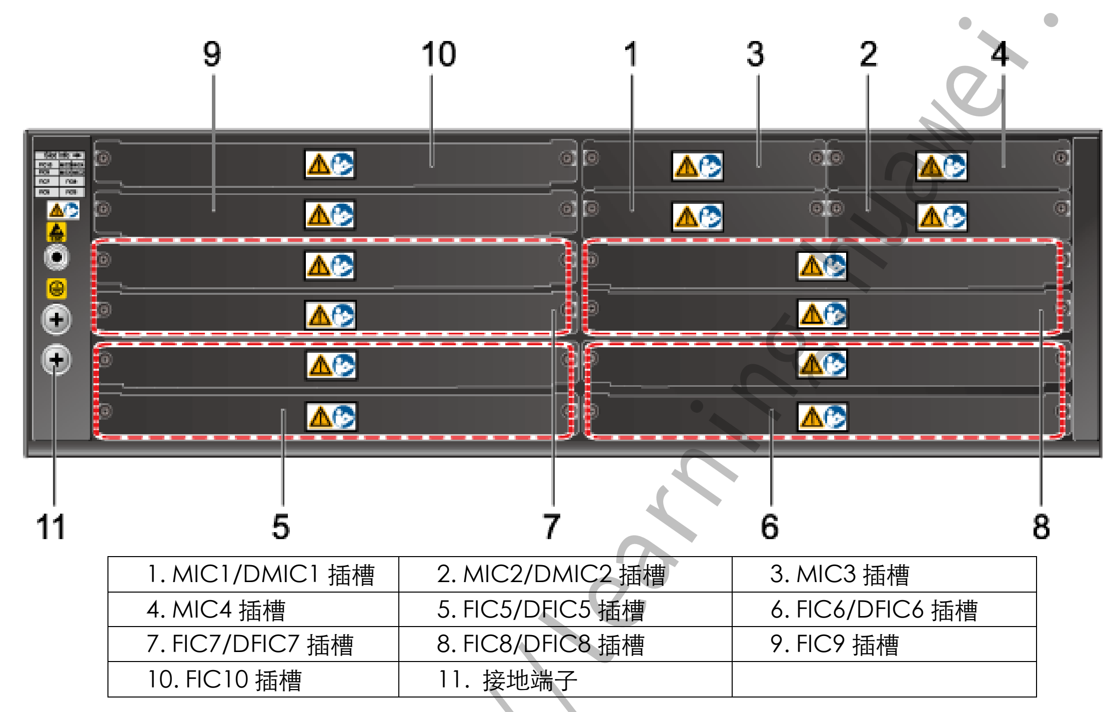


USG5150 前面板（交流机型）



1.防尘网	2. 指示灯	3.系统复位键
4. Console 接口	5. 闪存接口	6. USB2.0 接口
7. GE Combo 接口 0	8. GE Combo 接口 1	9. GE Combo 接口 2
10. GE Combo 接口 3	11. 风扇框	12. ESD 防静电插孔
13. 防尘挡板	14. 交流/直流电源模块 1	15.交流/直流电源模块 0

- 后面板



1. MIC1/DMIC1 插槽	2. MIC2/DMIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6/DFIC6 插槽
7. FIC7/DFIC7 插槽	8. FIC8/DFIC8 插槽	9. FIC9 插槽
10. FIC10 插槽	11. 接地端子	

- 槽位分布和排列顺序

USG5150 的 FIC5、FIC6、FIC7 和 FIC8 槽位除了可插入一个 DFIC 接口卡外，还可只在下半部分插入一个 FIC 接口卡。此时，为了防尘需要在 DFIC 槽位的上半部分安装一个假面板，以封闭后面板。如下图所示。

USG5150 槽位编号及排列顺序示意图

<table>
<tr><td>FIC10</td><td>MIC3</td><td>MIC4</td></tr>
<tr><td>FIC9</td><td>MIC1</td><td>MIC2</td></tr>
<tr><td>FIC7</td><td colspan="2">FIC8</td></tr>
<tr><td>FIC5</td><td colspan="2">FIC6</td></tr>
</table>

提示：FIC9 和 FIC10 两个槽位可以插入两个 FIC 接口卡，但不可以使用 DFIC 接口卡；FIC9 和 FIC10 两个槽位不支持 1GE 接口卡、4GE 接口卡、1GPON 接口卡、16POTS 接口卡和 32POTS 接口卡；

1.2.4 物理接口编号方法

设备物理接口采用的编号原则如下：

各接口按照从下到上，从左到右的顺序依次编号。物理接口编号为 interface-type X/0/Y，interface-type 为接口类型（如 Ethernet 等），X 表示槽位号，0 为板卡号，目前支持的接口卡没有子卡，所以此位均为 0。Y 表示接口序号。主板的槽位号为 0。

例如，USG 的 2 号槽位安装了 5FSW 接口卡，那么各接口的编号为：Ethernet2/0/0、Ethernet2/0/1、Ethernet2/0/2、Ethernet2/0/3、Ethernet2/0/4。

1.3 终端安全产品描述

1.3.1 TSM 产品概述

TSM，终端安全管理（Terminal Security Management）。为了解决企业内部网络管理失控的问题，保障企业内部网络的畅通、终端主机的安全和公司信息数据的安全，实现企业网络安全建设的目标，华为科技有限公司推出 TSM 这款产品，该产品为企业提供整合的内部网络安全解决方案，实现从终端到业务系统的控制和管理功能。

TSM 基于 TSM 代理为企业提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发和资产管理六大功能。其核心思想是建立网络准入控制机制，基本要素是安全检查、访问控制和安全修复。有效控制网络日渐增多的接入点，包括企业员工、外部访客、合作伙伴和临时雇员等对网络的访问，发现并隔离带有威胁的终端主机，提升网络防御安全威胁的能力。

1.3.2 TSM 系统部署

TSM 包括 TSM 管理中心、TSM 管理器、TSM 控制器、扫描器、安全接入控制网关、802.1x 交换机和 TSM 代理几个部件。

TSM 管理中心

TSM 管理中心是为分级式组网专门设立的组件，主要负责为 TSM 管理器分配 License、分配 Microsoft Windows 操作系统补丁模板、分配策略模板、分配软件分发任务。

TSM 管理中心的具体功能有：管理 TSM 管理器，管理 TSM 管理器的 License，管理策略模板，管理 Microsoft Windows 操作系统补丁，管理软件分发任务。

TSM 管理器

TSM 管理器是 TSM 的管理服务器。管理员通过 IE 浏览器登录 TSM 管理器进行日常维护操作。

TSM 管理器的主要功能包括：系统配置，组织人员管理，安全策略管理，补丁管理，软件分发，资产管理，公告管理，报表管理。

TSM 控制器

TSM 控制器是 TSM 的控制服务器。TSM 控制器主要负责验证终端用户的身份、对终端主机进行安全检查，以及与准入控制设备联动实现最小授权的访问控制等。

TSM 控制器的主要功能包括：向 TSM 代理、Web Agent 插件和 Web 客户端提供服务，与安全接入控制网关联动控制终端主机接入受控网络，与支持 802.1x 的交换机联动控制终端主机接入受控网络。

扫描器

扫描器的作用是发现和管理网络中现有的设备，尤其是已经安装 TSM 代理终端主机数量和未安装 TSM 代理的终端主机数量，在管理员制定或调整 TSM 代理的部署策略时作为参考的依据。

部署TSM代理是终端安全管理业务逐步推行的过程，按阶段分可分为试点和推广两个阶段，最终的目标是实现终端安全业务全覆盖。在终端安全管理业务逐步推行的过程中，管理员重点关注的是，如何确保所有的终端主机全部安装TSM代理，确保终端安全不会成为网络安全中最薄弱的环节。

扫描器是为了帮助管理员发现没有安装TSM代理的终端主机而开发的,主要功能有:通过扫描任务发现网络中的设备,能够识别已经安装TSM代理的终端主机和尚未安装TSM代理的终端主机，允许管理员标识需要安装TSM代理的终端主机和不需要安装TSM代理的终端主机，支持实时启动和停止扫描任务，支持周期性的扫描任务和一次性的扫描任务，支持按IP地址段和按ARP表两种方式发现设备，在发现新的设备接入受控网络和TSM代理被卸载时以告警邮件的方式提醒管理员，支持对设备进行分组管理。

安全接入控制网关

安全接入控制网关用于控制终端访问受控网络的权限，向隶属不同角色的终端用户和不同安全状况的终端用户开放不同的权限。

安全接入控制网关的主要功能包括: 根据TSM控制器反馈的信息开放终端用户访问受控网络的权限，防止外部非授权的终端用户访问企业的受控网络，防止内部合法但不安全的终端用户访问企业的受控网络，隔离连接到受控网络但没有进行安全认证的终端用户，支持逃生通道。

802.1x交换机

802.1x交换机的主要功能是对终端主机进行接入控制。通过端口控制技术，保证只有通过身份认证的终端主机才能接入受控网络，防止未经授权的终端主机接入受控网络。

TSM 服务器对应于 IEEE802.1x 的认证服务器系统，用户接入层设备则实现IEEE802.1x的接入控制单元，IEEE802.1x的用户接入系统集成在TSM代理中。

接入控制单元的每个物理端口内部有受控端口和非受控端口等逻辑划分。非受控端口始终处于双向连通状态，主要用来传递EAPOL协议帧，可保证随时接收用户接入系统发出的认证EAPOL报文。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

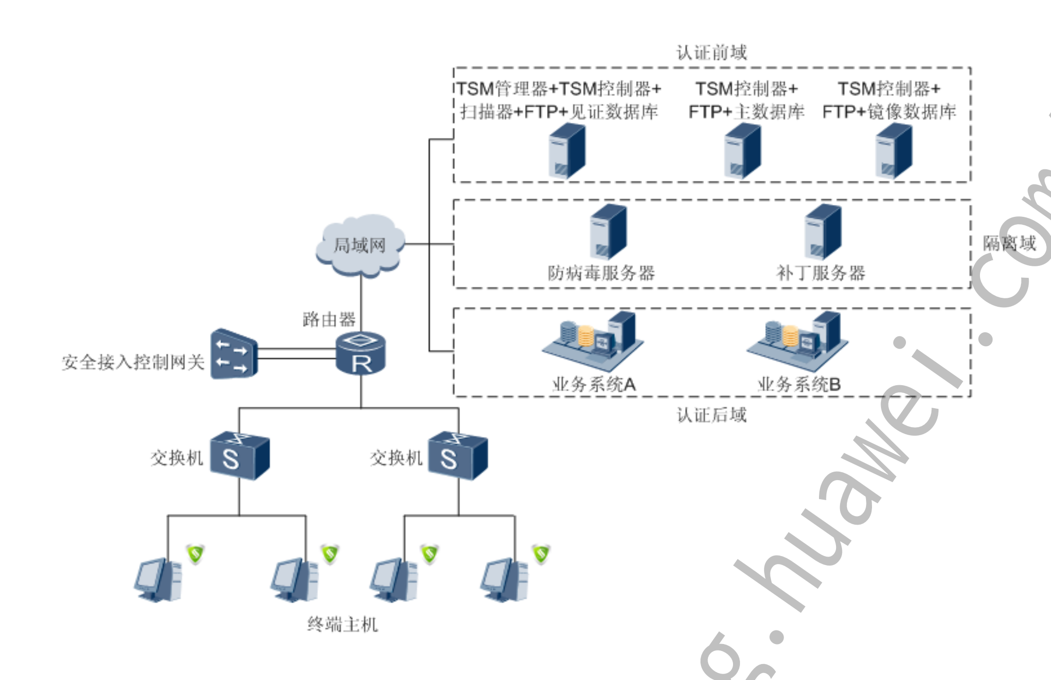
TSM代理

TSM代理是TSM中的一个组件，作为TSM的客户端安装在终端主机侧，负责与TSM管理器联动，实施管理员在TSM管理器定制的安全管理规则。

TSM代理根据安装过程的不同可以分为需要依照安装向导在终端主机安装的TSM代理和通过插件注册方式实现的Web Agent插件。

TSM代理的主要功能包括: 身份认证，安全认证，资产管理，补丁管理，软件分发，公告管理。

TSM系统部署组网图



1.3.3 TSM 性能指标

■ **TSM 控制器性能指标**

介绍 TSM 代理在进行身份认证和执行策略时的性能指标。

性能项目	性能指标
单台 TSM 控制器支持的最大终端用户数	10000
单台 TSM 控制器平均每分钟处理进行认证的终端主机数量	2500
终端主机上线成功率	在单台 TSM 控制器平均每分钟完成 2500 次身份认证的情况下，终端主机上线成功率大于 99%。
终端主机认证时延	在单台 TSM 控制器平均每分钟完成 2500 次身份认证的情况下，终端主机的认证时延小于等于 10s。
违规信息保存的最长时间	6 个月
与安全接入控制网关心跳检测时间	30s

■ **TSM 代理性能指标**

介绍 TSM 代理在进行身份认证和执行策略时的性能指标。

性能项目	性能指标
在不执行任何策略时 Microsoft Windows XP 的认证时间	≤3s
在不执行任何策略时 Microsoft Windows XP 最大内存占用	29MB
在执行所有策略时 Microsoft Windows XP 最大内存占用	35MB
在不执行任何策略时 Microsoft Windows Vista 的认证时间	≤3s
在不执行任何策略时 Microsoft Windows Vista 最大内存占用	30MB
在执行所有策略时 Microsoft Windows Vista 最大内存占用	36MB
CPU 平均占用率	15%
与 TSM 控制器之间的心跳检测时间	30s

1.4 图示



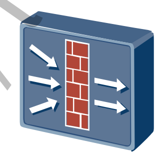
Internet



PC终端



网络云图



USG系列防火墙



便携PC终端



通用路由器



无线基站



服务器

2 如何登陆防火墙设备

2.1 通过Console口登录设备(超级终端)

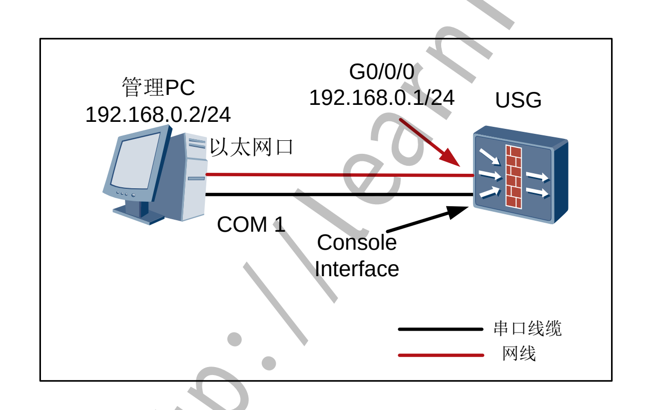
实验目的

在出厂配置下，PC 终端通过 Console 口登录设备，可实现对设备的管理和配置。。

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤

Step 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 在 PC 上运行终端仿真程序（以 Windows XP 的超级终端为例），选择“开始 > 程序 > 附件 > 通讯 > 超级终端”，显示“连接描述”对话框。

Step 3 在“名称”中输入 PC 与 USG 的连接名称，例如 COMM1；并在“图标”中选择任一图标，如图所示。

“连接描述”对话框（通过 Console 口登录）



Step 4 单击“确定”，显示“连接到”对话框。

Step 5 在“连接时使用”中选择 PC 与 USG 连接时使用的串口，例如 COM1，如图所示。



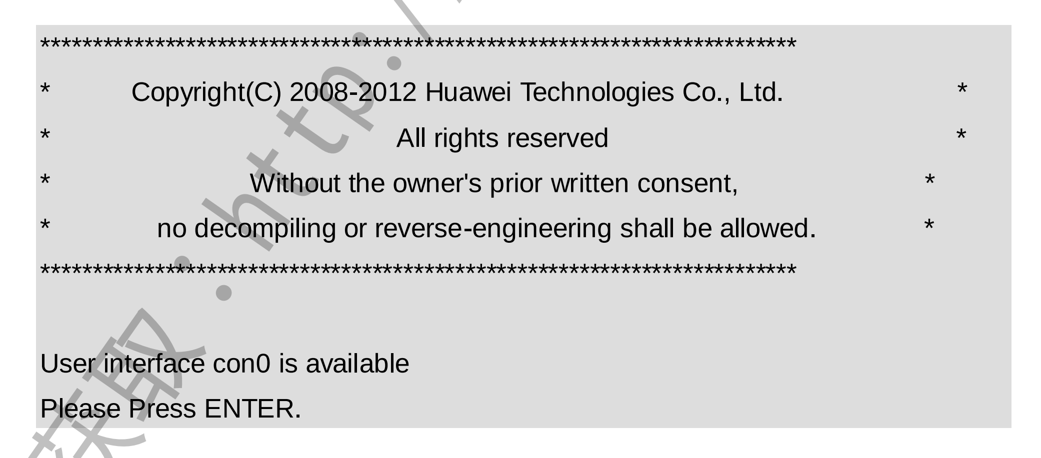
Step 6 单击“确定”，显示“COM1 属性”对话框。设置端口的通信参数，如图所示。



Step 7 单击“确定”或“还原为默认值（R）”。

Step 8 在 PC 仿真终端上，单击“Enter”，通过 USG 配置的认证方式后，按照提示输入用户名和密码后，即可进入用户视图，登录到设备上。

验证结果



```
**********************************************************************
*         Copyright(C) 2008-2012 Huawei Technologies Co., Ltd.          *
*                         All rights reserved                           *
*                Without the owner's prior written consent,             *
*           no decompiling or reverse-engineering shall be allowed.     *
**********************************************************************

User interface con0 is available
Please Press ENTER.
```

2.2 通过Console口登录设备(Putty)

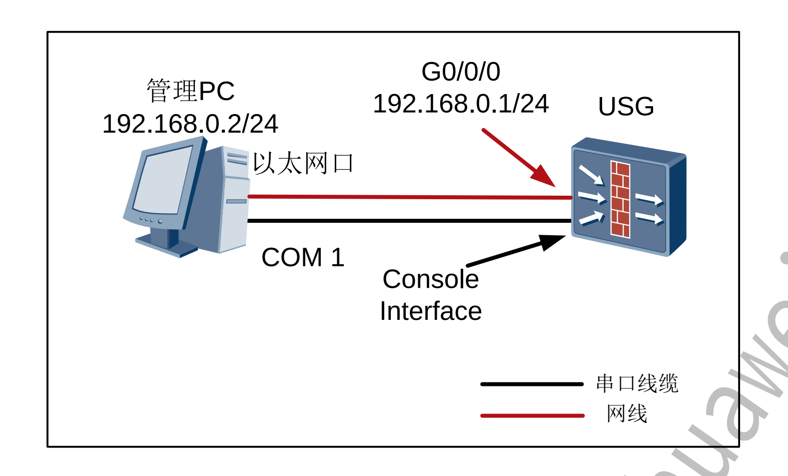
实验目的

在出厂配置下，PC 终端通过 Console 口登录设备，可实现对设备的管理和配置。。

组网设备

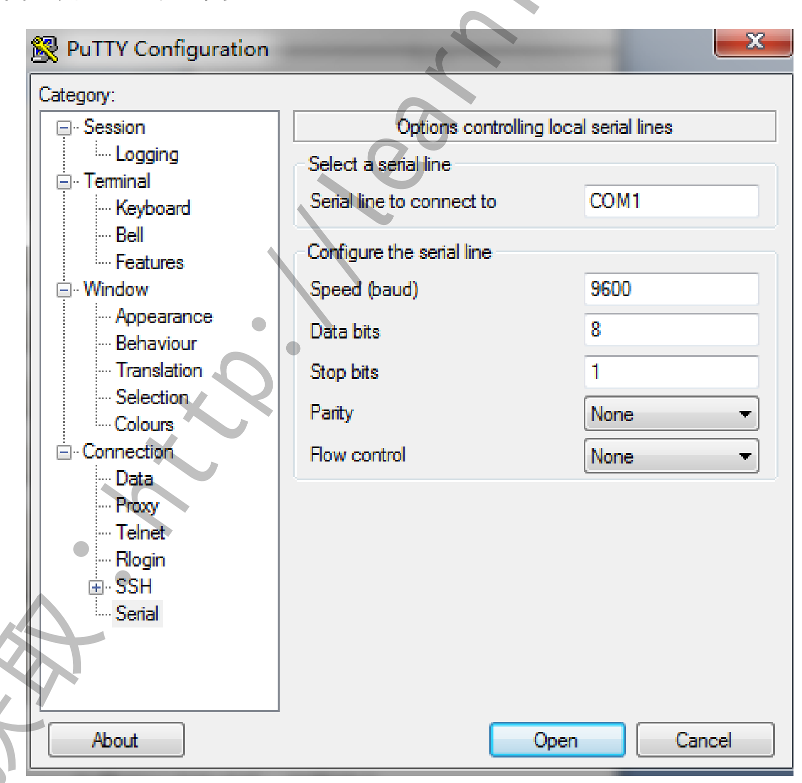
USG 防火墙一台，PC 机一台。

实验拓扑图

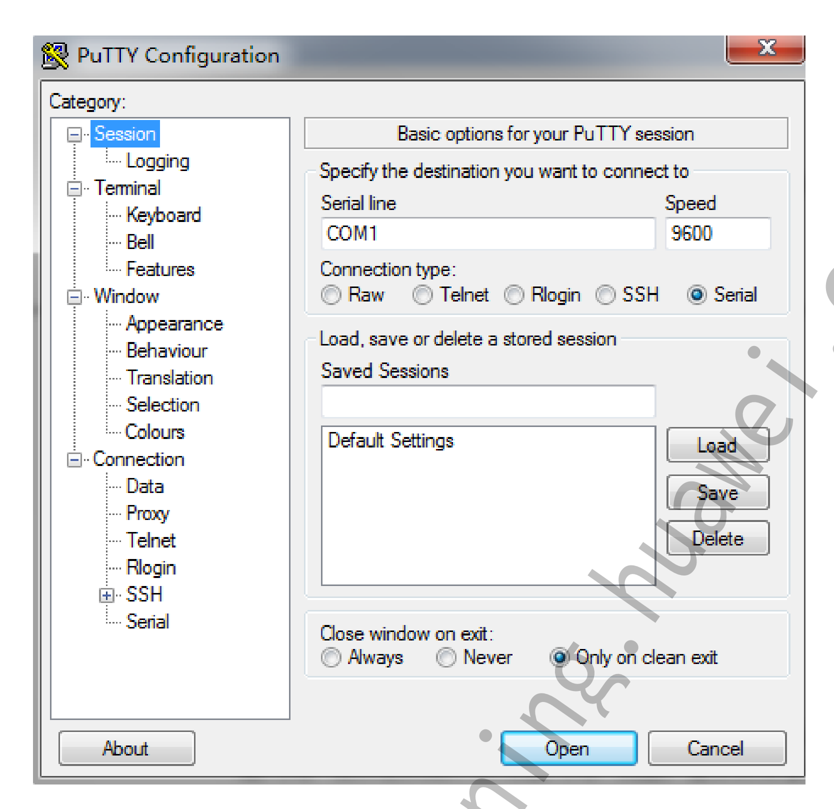


实验步骤

Step 1 下载 putty 软件到本地并双击运行该软件。配置通过串口连接设备的参数。具体参数配置如图所示。

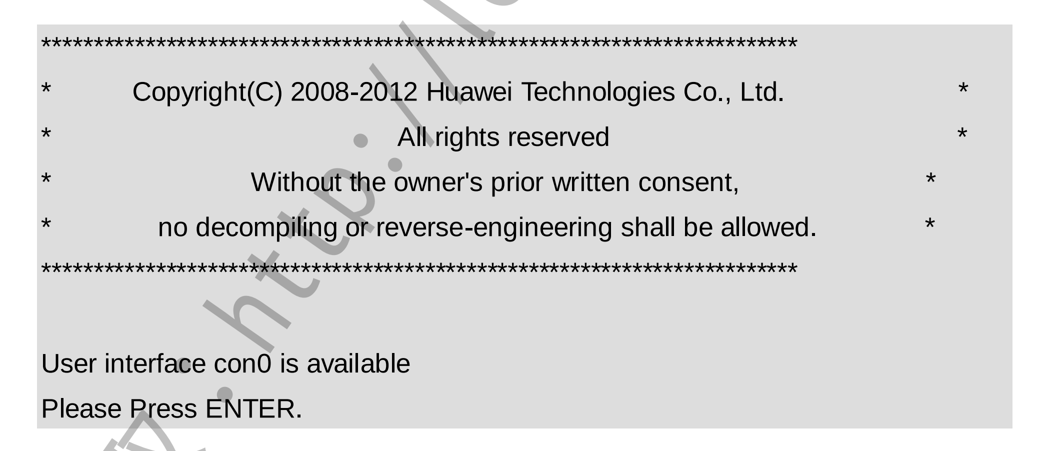


Step 2 单击“Open”，即可进入命令行配置界面。



Step 3 在 PC 仿真终端上，单击“Enter”，通过 USG 配置的认证方式后，按照提示输入用户名和密码后，即可进入用户视图，登录到设备上。

验证结果



2.3 通过Web方式登录设备（默认方式登录）

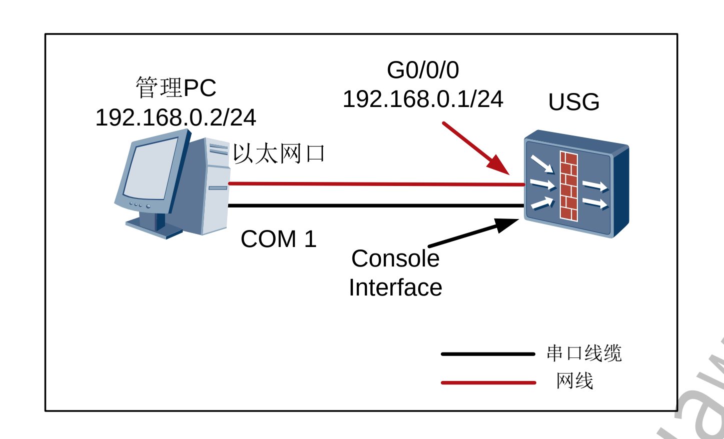
实验目的

在出厂配置下，PC 终端通过 Console 口登录设备，可实现对设备的管理和配置。。

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤

Step 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

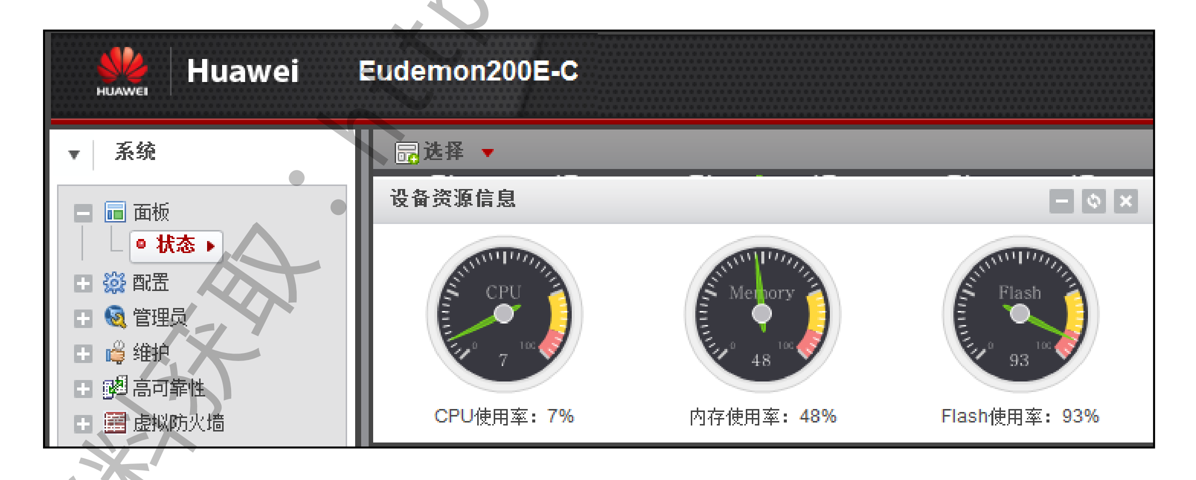
Step 2 PC 网卡和 USG G0/0/0 接口正常连接网线。

Step 3 配置 PC 的 IP 地址为 192.168.0.2/24。

Step 4 PC 的浏览器访问 http://192.168.0.1，输入用户名 admin，密码 Admin@123，检查是否可以登录设备。如果成功登录则表示配置成功，否则请检查配置。

Note：缺省情况下，设备的 G0/0/0 的 IP 地址是 192.168.0.1，并开启 HTTP 管理。用户可以通过用户名 admin，密码 Admin@123 登录。

验证结果



2.4 配置Telnet登录设备

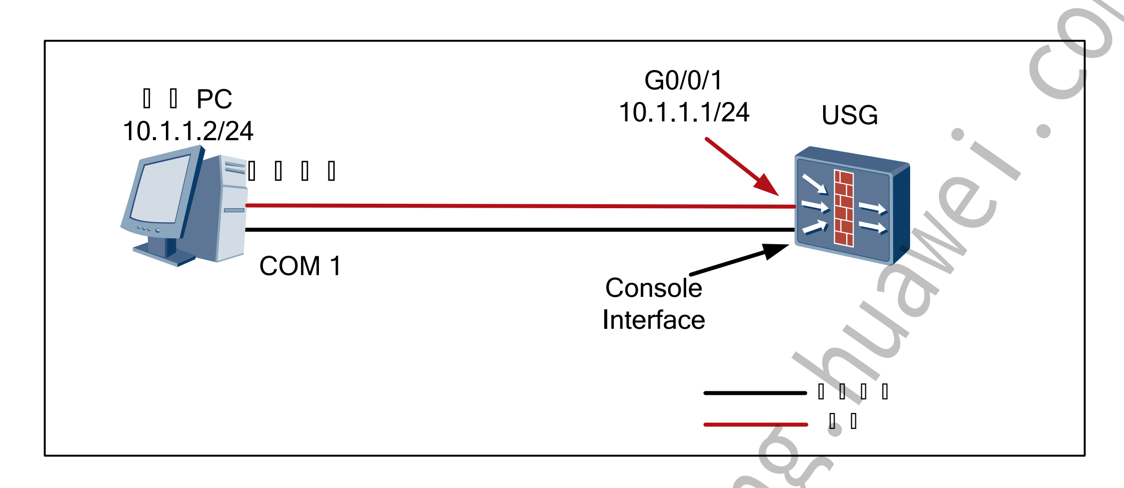
实验目的

通过配置使终端通过 Telnet 方式登录设备，实现对设备的配置和管理。

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤 – CLI

Step 1 通过 Console 口本地进入 USG 用户视图。参见 1.2 通过 Console 方式登陆防火墙设备。

Step 2 配置 USG 的接口 IP 地址。

以下面的情况为例进行配置：本地用户通过 Telnet 方式接入到 USG 千兆以太网接口 GigabitEthernet0/0/1，接口的 IP 地址为 10.1.1.1，子网掩码为 255.255.255.0。

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[USG-GigabitEthernet0/0/1] quit
```

Step 3 配置 USG 接口 Http 和 Https 设备管理。

```
<USG> system-view
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]service-manage enable
[USG-GigabitEthernet0/0/1]service-manage telnet permit
[USG-GigabitEthernet0/0/1]quit
```

Step 4 将 USG 接口 GigabitEthernet 0/0/1 加入安全区域。

```
[USG]firewall zone trust
[USG-zone-trust]add interface GigabitEthernet0/0/1
```

Step 5 将 USG 配置域间包过滤，以保证网络基本通信正常。

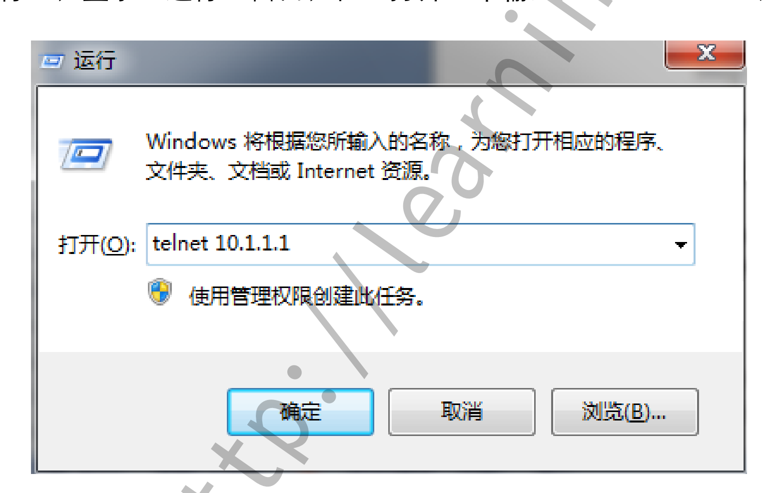
```
[USG]firewall packet-filter default permit interzone local trust
```

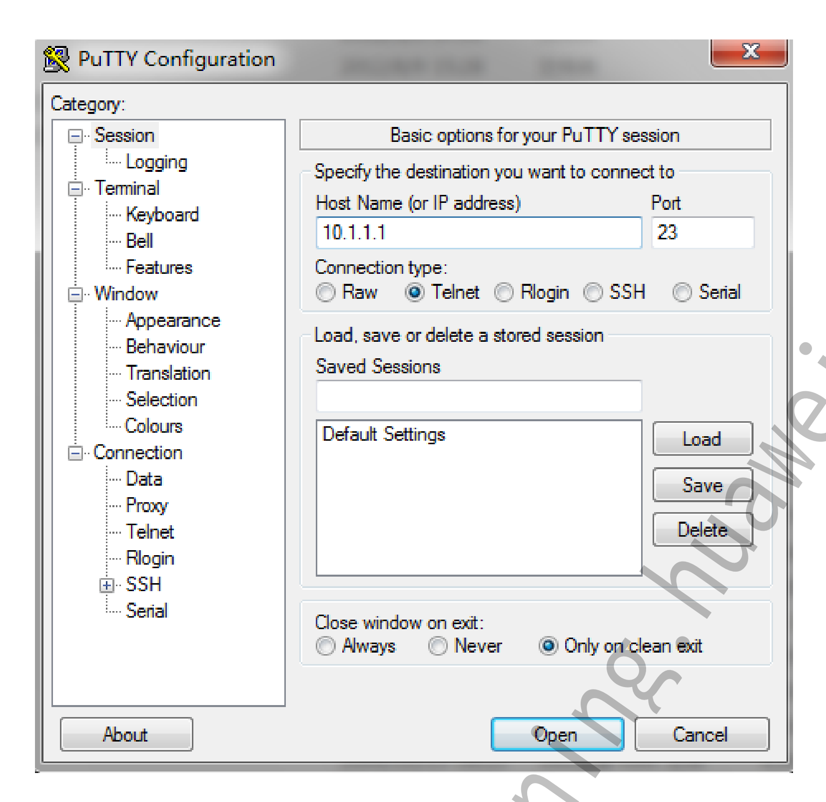
Step 6 配置 USG 的用户信息。

以下面的情况为例进行配置：配置 VTY（Virtual Type Terminal）用户接口的验证方式为 AAA，Telnet 用户名为 telnetuser，口令为 Admin@123@123，口令的存储方式为密文方式（cipher），级别为 level3。

```
<USG>system-view
[USG]user-interface vty 0 4
[USG-ui-vty0-4]authentication-mode aaa
[USG-ui-vty0-4]protocol inbound telnet
[USG-ui-vty0-4]quit
[USG]aaa
[USG-aaa]local-user telnetuser password cipherAdmin@123
[USG-aaa]local-user telnetuser service-type telnet
[USG-aaa]local-user telnetuser level 3
```

Step 7 在配置终端 PC 上运行 Telnet 程序或者 Putty，在 PC 上选择“开始 > 运行”，显示“运行”窗口，在“打开”中输入 telnet 10.1.1.1 如图所示。





Step 8 单击“确定”，开始连接 USG。

Step 9 通过 USG 配置的认证方式后，即可进入用户视图，登录到设备上。

实验步骤 – Web

Step 1 通过 Web 进入 USG 用户视图。参见 1.2 通过 Web 方式登陆防火墙设备。

Step 2 配置 USG 的 IP 地址。并配置 G0/0/1 接口 Telnet 设备管理。

网络 接口 接口

修改GigabitEthernet

接口名称 GigabitEthernet0/0/1 *

别名

VPN实例 public *

安全区域 trust

模式 路由 交换

连接类型 静态IP DHCP PPPoE

IP地址 10 . 1 . 1 . 1

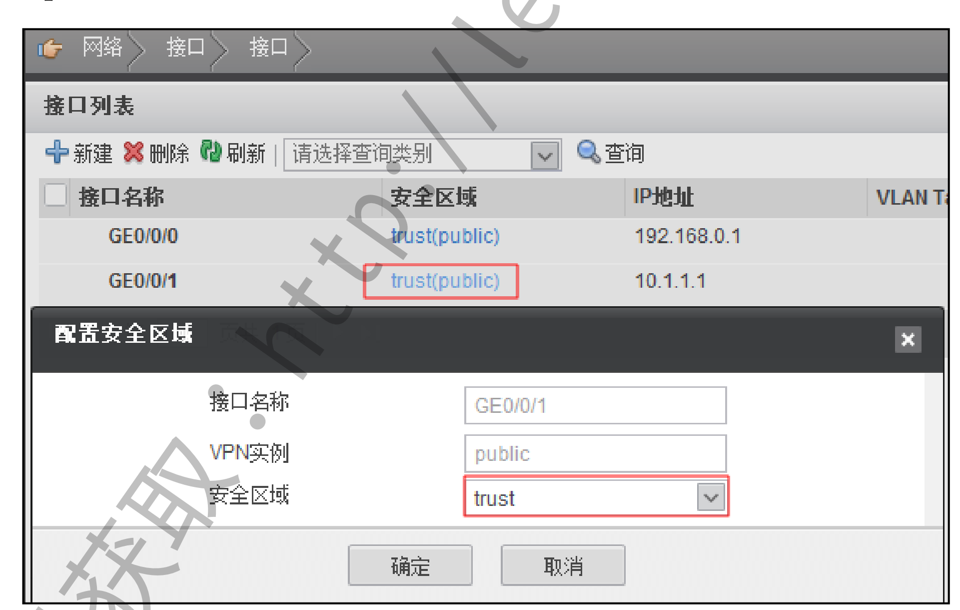
子网掩码 255 . 255 . 255 . 0

默认网关

NAT功能 启用

启用访问管理 HTTP HTTPS Ping SSH SNMP Telnet

Step 3 将 USG 接口 GigabitEthernet 0/0/1 加入安全区域。



Step 4 配置 USG 域间包过滤，保证管理数据通过 Trust 域到 Local 域



思考：配置 G0/0/1 接口 Telnet 设备管理的作用？容许数据 telnet 管理此端口。配置 USG 域间包过滤的作用？保证管理数据通过 Trust 域到 Local 域。

配置 telnet 用户。用户名 telnetuser，密码 Admin@123

系统 > 管理员 > 管理员

管理员密码管理配置

密码管理 启用

密码过期时间 90 <30-365>（天）

应用

管理员列表

新建 删除 刷新 按用户名查询 请输入用户名 查询

用户名	用户级别
admin	管理级

第 1 页共 1 页

系统 > 管理员 > 管理员

新建管理员

用户名 telnetuser *

密码 ••••••••• *(1-16个字符)

确认密码 ••••••••• *

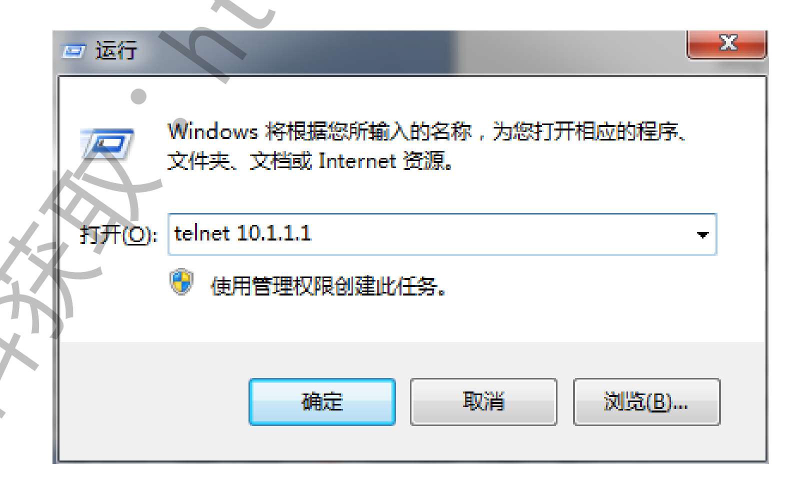
用户级别 管理级

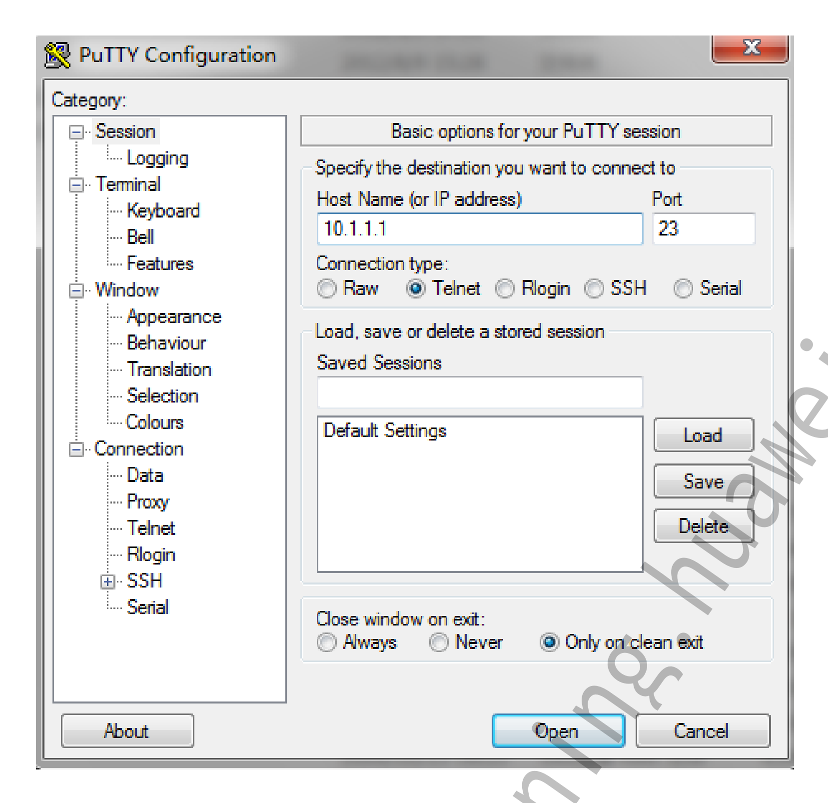
信任主机 #1

高级

应用 返回

Step 5 在配置终端 PC 上运行 Telnet 程序或者 Putty，在 PC 上选择“开始 > 运行”，显示“运行”窗口，在“打开”中输入 telnet 10.1.1.1 如图所示。

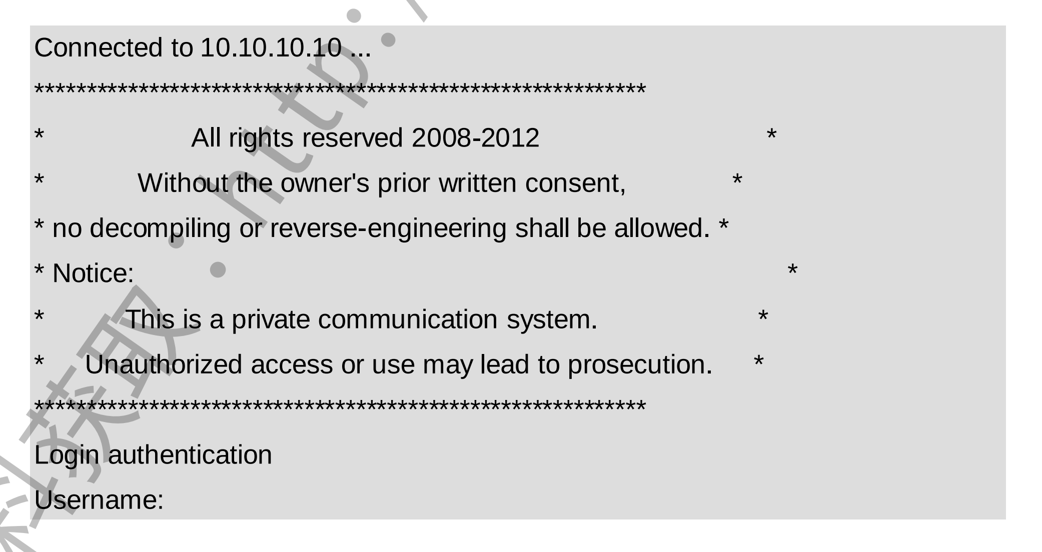




Step 6 单击“确定”，开始连接 USG。

Step 7 通过 USG 配置的认证方式后，即可进入用户视图，登录到设备上。

验证结果



```
Connected to 10.10.10.10 ...
************************************************************
*                All rights reserved 2008-2012              *
*          Without the owner's prior written consent,       *
* no decompiling or reverse-engineering shall be allowed. *
* Notice:                                                   *
*          This is a private communication system.          *
*    Unauthorized access or use may lead to prosecution.    *
************************************************************
Login authentication
Username:
```

2.5 配置Web方式登录设备

实验目的

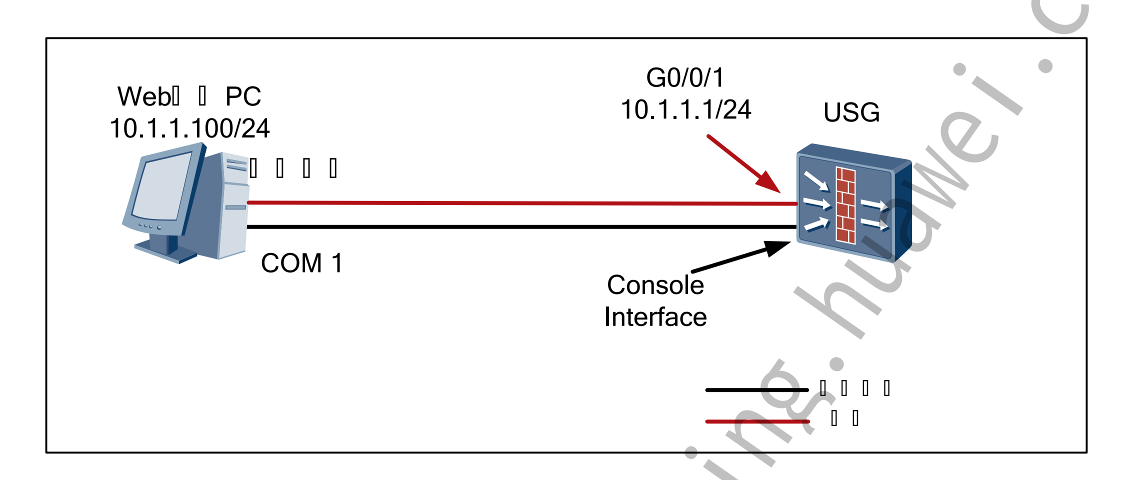
当用户通过出厂配置登陆了设备，需要通过 CLI 或者 Web 两种配置方式，设置 Web

设备管理参数，并开启 HTTP 或 HTTPS。

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤 - CLI

Step 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 配置 USG G0/0/1 的 IP 地址 10.1.1.1。

```
<USG>system-view
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]ip address 10.1.1.1 24
```

Step 3 配置 USG 接口 Http 和 Https 设备管理。

```
<USG>system-view
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]service-manage enable
[USG-GigabitEthernet0/0/1]service-manage http permit
[USG-GigabitEthernet0/0/1]service-manage https permit
[USG-GigabitEthernet0/0/1]quit
```

Step 4 将 USG 接口 GigabitEthernet 0/0/1 加入安全区域。

```
[USG]firewall zone trust
[USG-zone-trust]add interface GigabitEthernet0/0/1
```

Step 5 将 USG 配置域间包过滤，以保证网络基本通信正常。

```
[USG]firewall packet-filter default permit interzone local trust
```

Step 6 启动 Web 管理功能。

```
[USG]web-manager security enable port 2000
```

Note：执行 security 参数，是开启 https 管理。如 web-manager enable port 2000，不执行 security 参数，是开启 http 设备管理。

Note：不容许 Https 和 Http 管理使用相同的端口，这样配置会导致端口冲突。

Step 7 配置 Web 用户。

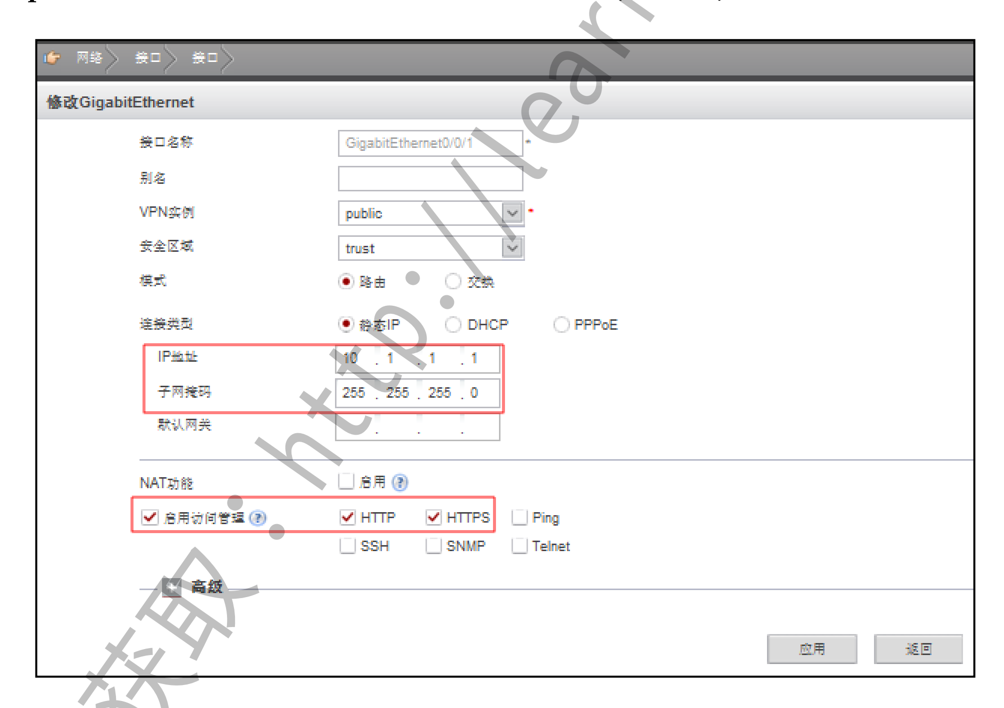
```
[USG]aaa
[USG-aaa]local-user webuser password cipher Admin@123
[USG-aaa]local-user webuser service-type web
[USG-aaa]local-user webuser level 3
```

Step 8 配置 PC 的 IP 地址为 10.1.1.100/24。 PC 的浏览器访问 https://10.1.1.1:2000。

实验步骤 － Web

Step 1 Web 登录设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 配置 USG 的 IP 地址。并配置 USG 接口 Http 和 Https 设备管理。



Step 3 将 USG 接口 GigabitEthernet 0/0/1 加入安全区域。

网络 接口 接口

接口列表

新建 删除 刷新 请选择查询类别 查询

接口名称	安全区域	IP地址	VLAN Ta
GE0/0/0	trust(public)	192.168.0.1	
GE0/0/1	trust(public)	10.1.1.1	

配置安全区域

接口名称 GE0/0/1

VPN实例 public

安全区域 trust

确定 取消

Step 4 配置 USG 域间包过滤，允许设备管理数据从 Trust 域到 Local 域通过。



Step 5 启动 Web 管理功能，根据客户需求启动 HTTP 或者 HTTPS 管理，以及设置端口号。



Step 6 配置 Web 用户。用户名 webuser，密码 Admin@123

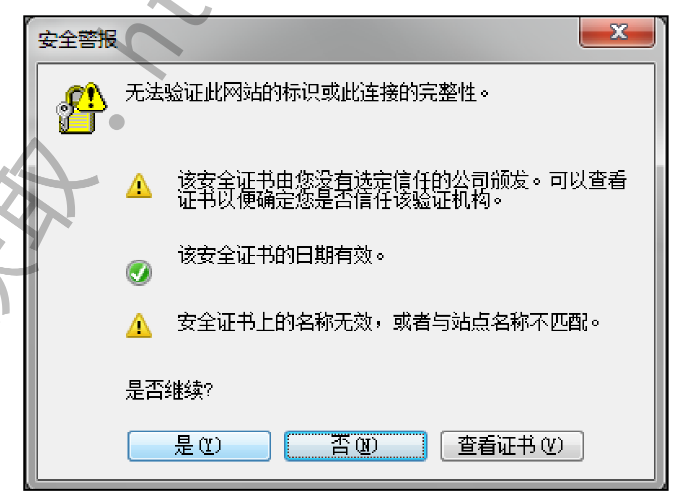




Step 7 配置PC的IP地址为10.1.1.100/24。PC的浏览器访问https://10.1.1.1:2000。

验证结果

安全证书警告，选择是继续。



2.6 配置SSH方式登录设备

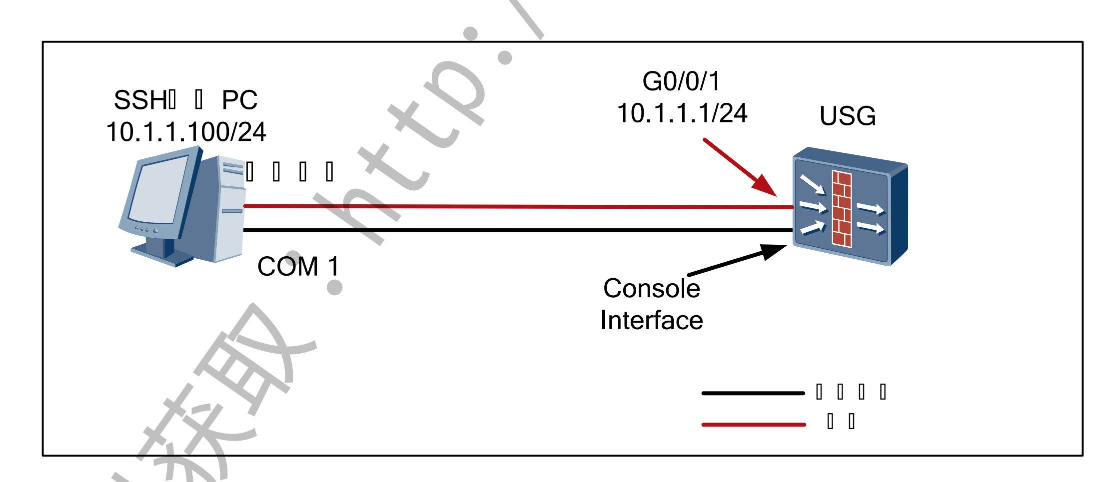
实验目的

当用户通过出厂配置登陆了设备，需要通过 CLI 或者 Web 两种配置方式，SSH 管理设备。

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤（CLI）

Step 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 配置 USG G0/0/1 的 IP 地址 10.1.1.1。（略）

Step 3 配置 USG 接口 SSH 设备管理。

```
<USG>system-view
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]service-manage enable
[USG-GigabitEthernet0/0/1]service-manage ssh permit
[USG-GigabitEthernet0/0/1]quit
```

Step 4 将 USG 接口 GigabitEthernet 0/0/1 加入安全区域。 （略）

Step 5 将 USG 配置域间包过滤，以保证网络基本通信正常。（略）

Step 6 配置 RSA 本地密钥对。

```
[USG]rsa local-key-pair create
The key name will be: USG_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
        It will take a few minutes.
Input the bits in the modulus[default = 512]:512
Generating keys...
..++++++++++++
...................................++++++++++++
.....++++++++
..++++++++
```

Step 7 配置 VTY 用户界面。

```
[USG]user-interface vty 0 4
[USG-ui-vty0-4]authentication-mode aaa
[USG-ui-vty0-4]protocol inbound ssh
[USG-ui-vty0-4]quit
```

Step 8 新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

```
[USG]ssh user client001
[USG]ssh user client001 authentication-type password
```

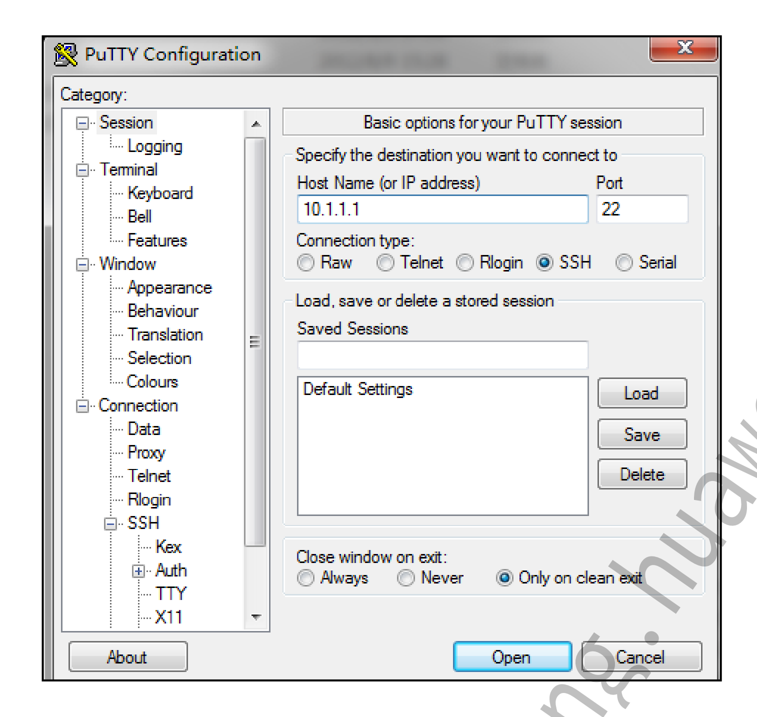
Step 9 配置 SSH 用户。

```
[USG]aaa
[USG-aaa]local-user sshuser password cipher Admin@123
[USG-aaa]local-user sshuser service-type ssh
[USG-aaa]local-user sshuser level 3
```

Step 10 配置 SSH 用户 sshuser 的服务方式为 STelnet，并启用 STelnet 服务。

```
[USG]ssh user sshuser service-type stelnet
[USG]stelnet server enable
```

Step 11 配置 PC 的 IP 地址为 10.1.1.100/24。 PC 通过 Putty SSH 访问设备。



实验步骤 - Web

Step 1 Web 登录设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 配置 USG 的 IP 地址。并配置 USG 接口 ssh 设备管理。



Step 3 将 USG 接口 GigabitEthernet 0/0/1 加入安全区域。 （略）

Step 4 配置 USG 域间包过滤，保证数据通过 Trust 域到 Local 域。（略）

Step 5 配置 SSH 用户。用户名 sshuser，密码 Admin@123

系统 > 管理员 > 管理员

管理员密码管理配置

密码管理 启用

密码过期时间 90 <30-365>（天）

应用

管理员列表

新建 删除 刷新 按用户名查询 请输入用户名 查询

用户名	用户级别
admin	管理级

第 1 页共 1 页

系统 > 管理员 > 管理员

新建管理员

用户名 sshuser *

密码 ********* *(1-16个字符)

确认密码 ********* *

用户级别 管理级

信任主机 #1

高级

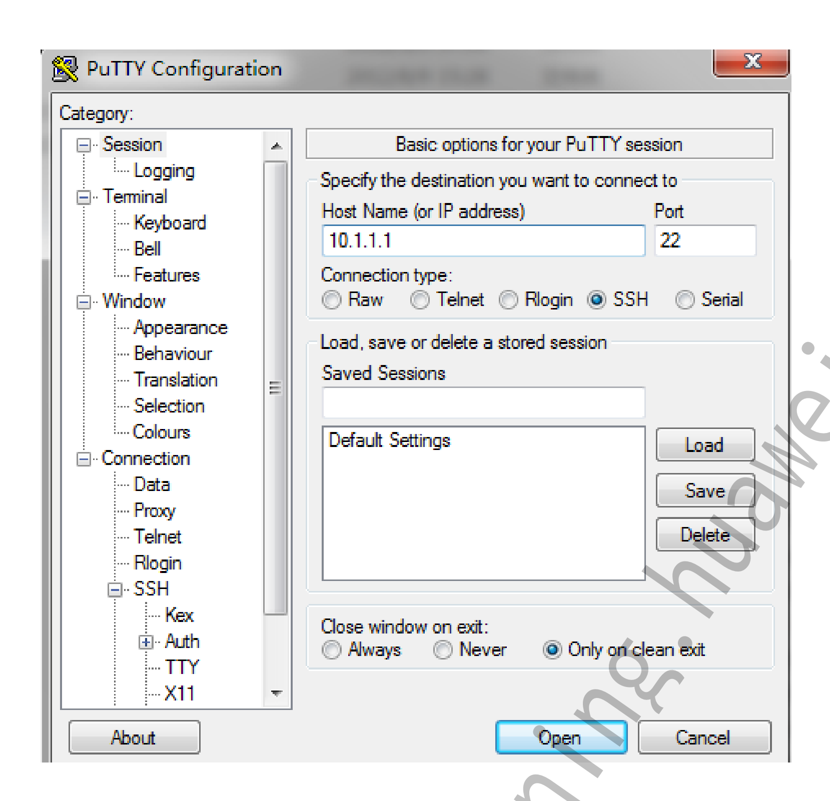
SSH认证方式 PASSWORD

应用 返回

Step 6 配置 SSH 用户的服务方式为 STelnet，并启用 STelnet 服务。



Step 7 配置 PC 的 IP 地址为 10.1.1.100/24。 PC 通过 Putty SSH 访问设备。



验证结果

输入用户名 sshuser 密码 Admin@123 登录设备

```
10.1.1.1 - PuTTY
login as: sshuser
sshuser@10.1.1.1's password:

***********************************************************
*          All rights reserved 2008-2012                  *
*      Without the owner's prior written consent,         *
* no decompiling or reverse-engineering shall be allowed. *
* Notice:                                                 *
*         This is a private communication system.         *
*   Unauthorized access or use may lead to prosecution.   *
***********************************************************

Note: The max number of VTY users is 5, and the current number
      of VTY users on line is 2.
Warning: Using default authentication method and password on console.
<USG>
<USG>
<USG>
```

3 防火墙基础配置

3.1 系统管理

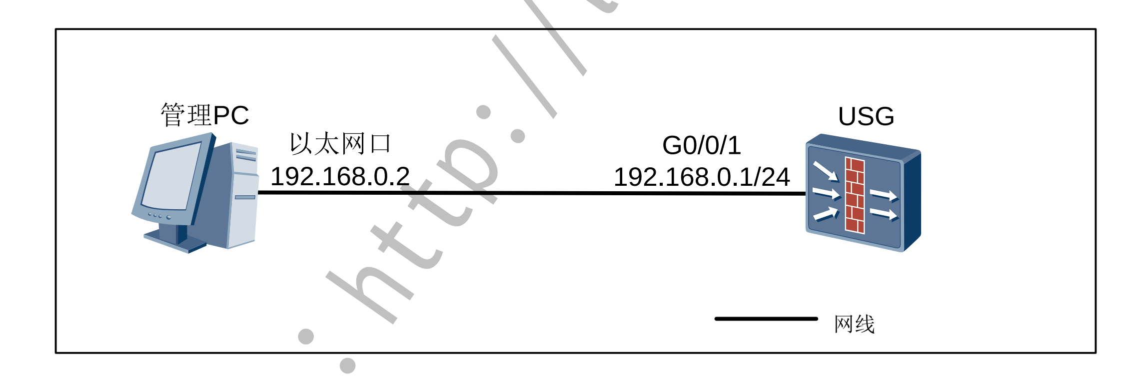
实验目的

配置设备主机名
配置时间
配置 SNMP 服务器
配置日志服务器
配置 License
配置文件的备份和恢复

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤（CLI）

Step 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 通过 Console，Telnet，SSH 等管理方式，登录到设备中。 实验步骤参考 1.1-1.6（略）。

Step 3 配置设备主机名

```
<USG>system-view
[USG]sysname USG_A
[USG_A]
```

Step 4 配置时间

```
<sysname>clock datetime 0:0:0 2009/01/01
```

Step 5 配置 SNMP V2c 服务器。SNMP 服务器是 192.168.1.2

```
<USG>system-view
[USG]snmp-agent sys-info version v2c        //设置 SNMP 版本号 V2c
[USG]snmp-agent community read public       //设置 SNMP 只读团体字 public
[USG]snmp-agent community write admin       //设置 SNMP 读写团体字 admin
[USG]snmp-agent trap enable     //设置 SNMP trap 功能
[USG]snmp-agent target-host trap address udp-domain 192.168.1.2 params
securityname swebUser v2c    //设置 SNMP trap 服务器
```

思考：Snmp Agent Trap 的作用是什么？

配置管理设备主动向网管服务器发送告警。如果不配置 Snmp Trap，Snmp 网管服务将只是周期性向被管理设备发送各种查询报文，设备返回查询数据。

Step 6 配置日志服务器

查看信息中心是否使能，使能后才能记录日志信息，默认是使能的。

```
[sysname]display info-center
Information Center:enabled
```

开启信息中心。

```
[sysname]info-center enable
```

配置日志服务器 IP 地址和发送日志信息的源接口。

```
[sysname]info-center loghost 192.168.1.10
[sysname]info-center loghost source GE0/0/1
```

Step 7 配置 License

```
[sysname]license file hda1:/license.dat
```

Step 8 配置备份和恢复

设备做 FTP Server 的方式

//配置网络连接、IP 地址、接口安全区域及包过滤。（略）

//开启设备的 FTP 功能并配置 FTP 用户名、密码及 FTP 路径。

```
<sysname>system-view
[sysname]ftp server enable
Info:Start FTP server
[sysname]aaa
[sysname-aaa]local-user ftpuser password cipher Ftppass#
[sysname-aaa]local-user ftpuser service-type ftp
[sysname-aaa]local-user ftpuser level 3
[sysname-aaa]local-user ftpuser ftp-directory hda1:/
```

//从配置终端使用 ftp 命令登录到设备上。

备份： 使用 get 命令从设备下载文件到 PC。

这里以安装 Windows 操作系统的 PC 为例："开始 > 运行"，输入 cmd 后单击 "确定"。

```
C:\Documents and Settings\Administrator> ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User (192.168.0.1:(none)): ftpuser
331 Password required for ftpuser.
Password:
230 User logged in.
ftp> get vrpcfg.cfg
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.cfg.
226 Transfer complete.
ftp: 收到 5203 字节，用时 0.01Seconds 346.87Kbytes/sec.
ftp> lcd
Local directory now C:\Documents and Settings\Administrator.
ftp>
```

恢复：

恢复的步骤和备份的步骤类似，但是有两点不同点。

//恢复使用 put 命令将文件上传到设备上。

```
ftp> put vrpcfg.cfg
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.cfg.
226 Transfer complete.
ftp: 发送 5203 字节，用时 0.00Seconds 5203000.00Kbytes/sec.
```

// **在 USG 设备中配置命令行**，配置设备下次启动使用的配置文件。

```
<sysname> startup saved-configuration vrpcfg.cfg
```

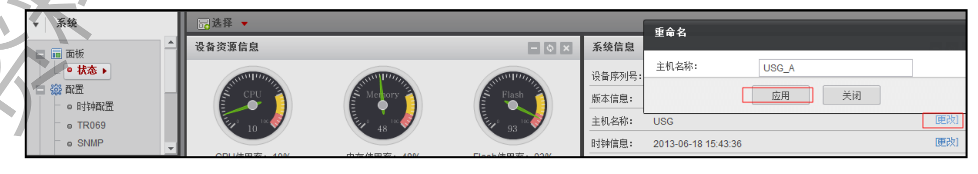
实验步骤（Web）

Step 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 通过 Web 管理方式，登录到设备中。 实验步骤参考 1.5（略）。

Step 3 配置设备主机名 USG_A。

选择 "系统 > 面板 > 状态 > 系统信息 > 主机名称"。



Step 4 配置时间

选择 "系统 > 配置 > 时钟配置"。

系统 > 配置 > 时钟配置

配置系统时间

配置方式 手动配置时间

时区 (+8)北京，重庆，广州，上海，香

日期 2013/06/18

系统时间 15:34:57

根据夏时制自动调节时钟

应用 刷新

Step 5 配置 SNMP V2c 服务器。SNMP 服务器是 192.168.1.2

选择“系统 > 配置 >SNMP”。设置如图所示：

系统 > 配置 > SNMP

配置SNMP

SNMP版本 v1 v2c v3

SNMP只读团体名 ••••••

SNMP读写团体名 •••••••

Trap接收主机：端口1 192 . 168 . 1 . 2 : 162 <0-65535> Trap口令 swebUser

Trap报文源地址 ----- NONE -----

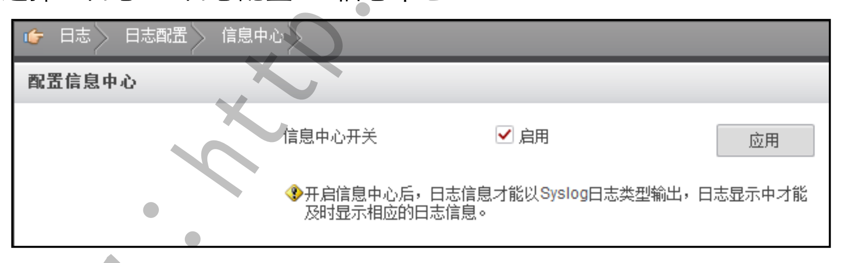
设备位置 China

联系信息 R&D Huawei Technolog

应用

Step 6 配置日志服务器

//查看信息中心是否使能，使能后才能记录日志信息，默认是使能的。
选择“日志 > 日志配置 > 信息中心”。



//配置日志服务器 IP 地址和发送日志信息的源接口。
选择“日志 > 日志配置 > Syslog 配置”。设置源接口 GE0/0/1,并新建日志主机 192.168.1.10。





Step 7 配置 License

选择导入 PC 本地的 License 文件，并选择激活。License 具体的信息在 License 资源表中显示。



License资源	状态	
虚拟防火墙	已授权（15个虚拟防火墙）	
SSL_VPN	已授权（10个并发用户）	
入侵防御	已授权（过期时间：2014/05/06）	
版本号：	20130502.011	[升级配置]
签名库版本：	20130502.011（升级时间：15:32:00 2013/06/18...	
反病毒	已授权（过期时间：2014/05/06）	
版本号：	20130505.008	[升级配置]
签名库版本：	20130505.008（升级时间：15:38:00 2013/06/18...	
垃圾邮件过滤	已授权（过期时间：2014/05/06）	
URL预定义分类查询	已授权（过期时间：2017/05/06）	[激活]

Step 8 配置备份和恢复

通过 Web 备份和恢复配置

备份：

//在菜单导航树中选择“系统 > 维护 > 配置管理”进入配置管理界面。

查看当前的配置文件是 vrpcfg.zip。

单击“选择”按钮，进入配置文件管理界面：



//单击待备份的配置文件对应的下载图标：

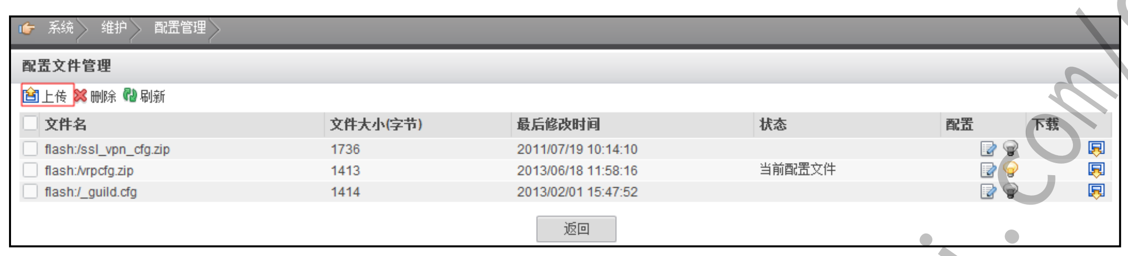
此配置文件当前正在使用，点击 下载配置文件到本地。



文件名	文件大小(字节)	最后修改时间	状态	配置	下载
flash:/ssl_vpn_cfg.zip	1736	2011/07/19 10:14:10			
flash:/vrpcfg.zip	1413	2013/06/18 11:58:16	当前配置文件		
flash:/_guild.cfg	1414	2013/02/01 15:47:52			

恢复：

//单击按钮进入上传文件界面。



//单击“浏览”按钮选择本地的配置文件后，选择“OK”后，设备会将文件上传到设备中。



//设置上次配置文件为下次启动文件。上传文件所在行上单击 图标，图标变成 。

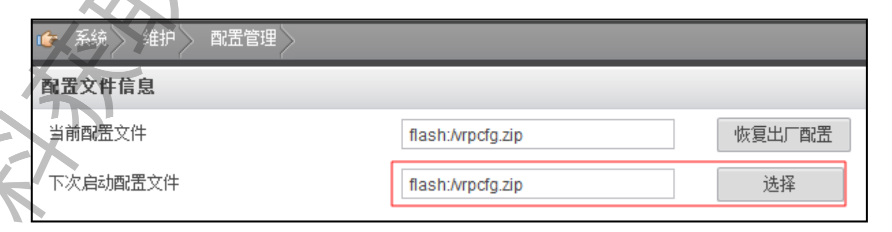
//重新启动设备，使配置文件生效。

选择“系统 > 维护 > 系统重启”，输入用户名密码，重启设备。



验证结果

选择“系统 > 维护 > 配置管理”查看下一次启动的配置文件。



4 防火墙安全转发策略

4.1 基于IP地址的转发策略

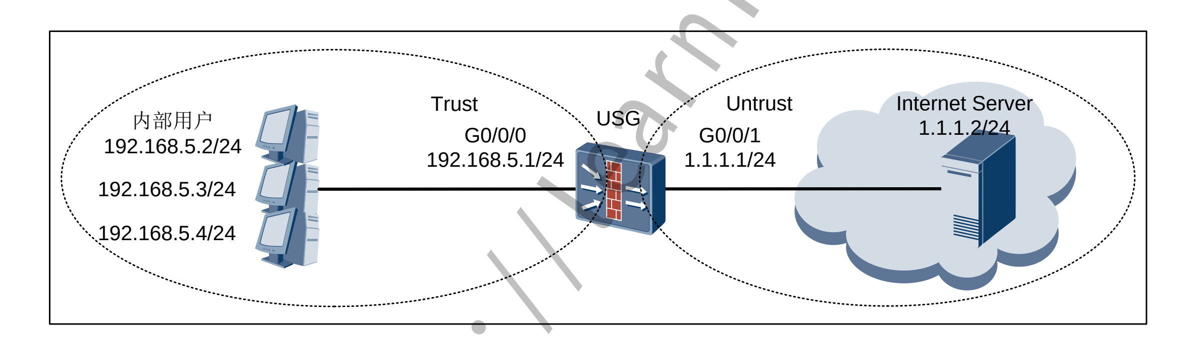
实验目的

介绍最基本的通过 IP 地址控制访问权限的举例。

组网设备

USG 防火墙一台，PC 机两台。

实验拓扑图



实验步骤 - CLI

Step 1 配置各个接口的 IP，并加入相应的安全区域。

```
<USG>system-view
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/2]ip address 192.168.5.1 24
[USG-GigabitEthernet0/0/2]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/3]ip address 1.1.1.1 24
[USG-GigabitEthernet0/0/3]quit
[USG]firewall zone trust
[USG-zone-trust]add interface GigabitEthernet 0/0/0
[USG-zone-trust]quit
[USG]firewall zone untrust
[USG-zone-untrust]add interface GigabitEthernet0/0/1
[USG-zone-untrust]quit
```

Step 2 配置名称为 ip_deny 的地址集，将几个不允许上网的 IP 地址加入地址集。

```
[USG]ip address-set ip_deny type object
[USG-object-address-set-ip_deny]address 192.168.5.2 0
[USG-object-address-set-ip_deny]address 192.168.5.3 0
[USG-object-address-set-ip_deny]address 192.168.5.6 0
[USG-object-address-set-ip_deny]quit
```

Step 3 创建拒绝特殊的几个 IP 地址访问 Internet 的转发策略。

```
[USG]policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound]policy 0
[USG-policy-interzone-trust-untrust-outbound-0]policy source address-set
ip_deny
[USG-policy-interzone-trust-untrust-outbound-0]action deny
[USG-policy-interzone-trust-untrust-outbound-0]quit
```

Step 4 创建允许其他属于 192.168.5.0/24 这个网段的 PC 访问 Internet 的转发策略。

```
[USG-policy-interzone-trust-untrust-outbound]policy 1
[USG-policy-interzone-trust-untrust-outbound-1]policy source 192.168.5.0 mask
24
[USG-policy-interzone-trust-untrust-outbound-1]action permit
[USG-policy-interzone-trust-untrust-outbound-1]quit
[USG-policy-interzone-trust-untrust-outbound]quit
```

Step 5 关闭缺省包过滤。

```
[USG] firewall packet-filter default deny interzone trust untrust
```

思考：为何要将缺省包过滤关闭，如果不关闭会有怎样的结果。

实验步骤 - Web

Step 1 配置各个接口的 IP，并加入相应的安全区域。如图所示：

网络 > 接口 > 接口

修改GigabitEthernet

接口名称	GigabitEthernet0/0/0 *
别名	
VPN实例	public *
安全区域	trust
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	192 . 168 . 5 . 1
子网掩码	255 . 255 . 255 . 0
默认网关	. . .

重复上述步骤配置接口 GigabitEthernet 0/0/1。

网络 > 接口 > 接口

修改GigabitEthernet

接口名称	GigabitEthernet0/0/1 *
别名	
VPN实例	public *
安全区域	untrust
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	1 . 1 . 1 . 1
子网掩码	255 . 255 . 255 . 0
默认网关	. . .

Step 2 配置名称为 ip_deny 的地址集，将几个不允许上网的 IP 地址加入地址集。选择“防火墙 > 地址 > 地址组”。 在“地址组列表”中单击，进入“新建地址组”界面。 配置地址组的名称和描述信息。

子网/IP范围	描述
192.168.5.2/32	
192.168.5.3/32	
192.168.5.6/32	

Step 3 创建拒绝特殊的几个 IP 地址访问 Internet 的转发策略。 选择“防火墙 > 安全策略 > 转发策略”。

源安全区域	trust	*
目的安全区域	untrust	*
源地址	deny_ip	多选
目的地址	请选择或输入IP地址	多选
用户	请选择用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	deny	*
描述		

Step 4 创建允许 192.168.5.0/24 这个网段访问 Internet 的转发策略。

源安全区域	trust	*
目的安全区域	untrust	*
源地址	192.168.5.0/24	多选
目的地址	请选择或输入IP地址	多选
用户	any	多选
服务	请选择服务	多选
时间段	all	
动作	permit	*
描述		

Step 5 关闭缺省包过滤。



思考：为何要将缺省包过滤关闭，如果不关闭会有怎样的结果。

验证结果

验证 192.168.5.2、192.168.5.3 和 192.168.5.6 这 3 台 PC 访问 Internet 是否被拒绝。

验证 192.168.5.0/24 中的其他 IP 地址是否可以正常访问 Internet。

5 网络地址转换实验

5.1 NAT Outbound实验

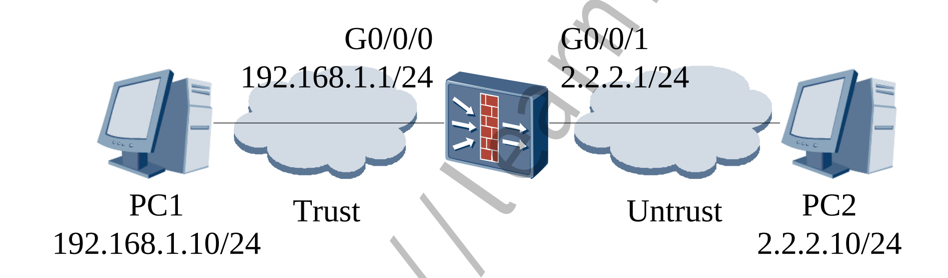
实验目的

通过本实验，你将了解 NAT outbound 的工作原理及详细配置。

组网设备

USG 防火墙一台，PC 机两台。

实验拓扑图



实验步骤 - CLI

Step 1 配置 PC1 和 PC2 的 IP 地址分别为 192.168.1.10/24 和 2.2.2.10/24。

Step 2 设置防火墙 GE0/0/0 和 GE0/0/1 的 IP 地址。

```
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0]ip address 192.168.1.1 255.255.255.0
[USG-GigabitEthernet0/0/0]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet0/0/1]quit
[USG]
```

Step 3 将接口加入防火墙安全区域。(GE0/0/0 加入 trust 区域，GE0/0/1 加入 untrust 区域)

```
[USG]firewall zone trust
[USG-zone-trust]add interface GigabitEthernet 0/0/0
```

```
[USG-zone-trust]quit
[USG]firewall zone untrust
[USG-zone-untrust]add interface GigabitEthernet 0/0/1
[USG-zone-untrust]quit
```

Step 4 配置域间包过滤策略。

```
[USG]policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound-0]policy 0
[USG-policy-interzone-trust-untrust-outbound-0]action permit
[USG-policy-interzone-trust-untrust-outbound-0]policy source 192.168.1.0 mask
24
```

Step 5 配置 NAT 地址池，公网地址范围为 2.2.2.2—2.2.2.5。

```
[USG]nat address-group 1 2.2.2.2 2.2.2.5
```

Step 6 配置 NAT policy。

```
[USG]nat-policy interzone trust untrust outbound
[USG-nat-policy-interzone-trust-untrust-outbound]policy 1
[USG-nat-policy-interzone-trust-untrust-outbound-1]action source-nat
[USG-nat-policy-interzone-trust-untrust-outbound-1]policy destination 2.2.2.10 0
.0.0.255
[USG-nat-policy-interzone-trust-untrust-outbound-1]address-group 1
[USG-nat-policy-interzone-trust-untrust-outbound-1]policy source 192.168.1.10
0.0.0.255
[USG-nat-policy-interzone-trust-untrust-outbound-1]quit
[USG-nat-policy-interzone-trust-untrust-outbound]quit
```

实验步骤 - Web

Step 1 配置 PC1 和 PC2 的 IP 地址分别为 192.168.1.10/24 和 2.2.2.10/24。

Step 2 设置防火墙 GE0/0/0 和 GE0/0/1 的 IP 地址。选择“网络 > 接口 > 接口”。在“接口列表”中单击各接口对应的 。配置如下图所示：配置完成后单击“应用”。

接口名称	GigabitEthernet0/0/0 *	
别名		
VPN实例	public *	
安全区域	trust	
模式	◉ 路由 ○ 交换	
连接类型	◉ 静态IP ○ DHCP ○ PPPoE	
IP地址	192 . 168 . 1 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

接口名称	GigabitEthernet0/0/1 *	
别名		
VPN实例	public *	
安全区域	untrust	
模式	◉ 路由 ○ 交换	
连接类型	◉ 静态IP ○ DHCP ○ PPPoE	
IP地址	2 . 2 . 2 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

Step 3 配置域间包过滤策略。选择“防火墙 > 安全策略 > 转发策略”。选择“转发策略”页签。在“转发策略列表”中单击 ✚。配置如下图所示：配置完成后单击“应用”。

源安全区域	trust *	
目的安全区域	untrust *	
源地址	192.168.1.10/24	多选
目的地址	2.2.2.10/24	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

Step 4 配置 NAT 地址池，公网地址范围为 2.2.2.2—2.2.2.5。选择“防火墙 > NAT > 源 NAT”。选择“NAT 地址池”页签。在“NAT 地址池列表”中单击 ➕。配置如下图所示：配置完成后单击“应用”。



Step 5 配置 NAT policy。选择“防火墙 > NAT > 源 NAT”。选择“源 NAT”页签。在“源 NAT 策略列表”中单击 ➕。配置如下图所示，配置完成后单击“应用”。

源安全区域	trust *	
目的安全区域	untrust *	
源地址	192.168.1.10/24	多选
目的地址	请选择或输入IP地址	多选
动作	NAT转换 *	
描述		
将源地址转换为	● 地址池中的地址	○ 接口IP地址
地址池	1 *	
	☑ 允许端口地址转换	

验证结果

查看 nat-policy 配置

```
[USG]dis nat-policy interzone trust untrust outbound
nat-policy interzone trust untrust outbound
 policy 1 (0 times matched)
  action source-nat
  policy service service-set ip
  policy source 192.168.1.0 0.0.0.255
  policy destination 2.2.2.0 0.0.0.255
  address-group 1
```

从 PC1 ping PC2 地址

```
PC1>ping 2.2.2.10
Ping 2.2.2.10: 32 data bytes, Press Ctrl_C to break
From 2.2.2.10: bytes=32 seq=1 ttl=127 time=79 ms
From 2.2.2.10: bytes=32 seq=2 ttl=127 time=31 ms
From 2.2.2.10: bytes=32 seq=3 ttl=127 time=94 ms
From 2.2.2.10: bytes=32 seq=4 ttl=127 time=62 ms
From 2.2.2.10: bytes=32 seq=5 ttl=127 time=94 ms
--- 2.2.2.10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/72/94 ms
```

使用 display firewall session table 命令查看 NAT 转换情况：

```
[USG]dis firewall session table
Current Total Sessions : 15
icmp  VPN:public --> public
192.168.1.10:45346[2.2.2.5:45346]-->2.2.2.10:2048
icmp  VPN:public --> public
192.168.1.10:45602[2.2.2.5:45602]-->2.2.2.10:2048
icmp  VPN:public --> public
192.168.1.10:45858[2.2.2.5:45858]-->2.2.2.10:2048
icmp  VPN:public --> public
192.168.1.10:46114[2.2.2.5:46114]-->2.2.2.10:2048
icmp  VPN:public --> public
192.168.1.10:46370[2.2.2.5:46370]-->2.2.2.10:2048
```

可以看到，防火墙将源地址 192.168.1.10 转换成了 NAT 地址池中的 2.2.2.5 与 PC2 进行通信。

5.2 NAT Server & NAT Inbound实验

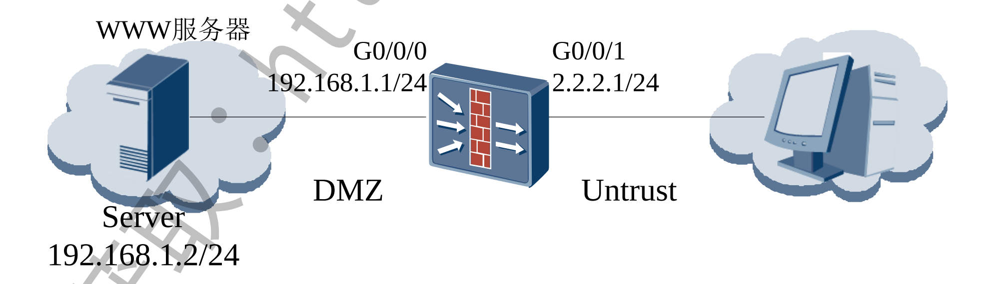
实验目的

学会配置 NAT Server 和 NAT inbound.

组网设备

USG 防火墙一台，PC 机一台，服务器一台。

实验拓扑图



实验步骤 – CLI

Step 1 设置 server 地址和 PC 地址。

Step 2 设置防火墙 GE0/0/0 和 GE0/0/1 的 IP 地址。

```
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0]ip address 192.168.1.1 255.255.255.0
[USG-GigabitEthernet0/0/0]quit
[USG]interface GigabitEthernet 0/0/1
```

```
[USG-GigabitEthernet0/0/1]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet0/0/1]quit
[USG]
```

Step 3 将接口加入防火墙安全区域。(GE0/0/0 加入 DMZ 区域,GE0/0/1 加入 untrust 区域)

```
[USG]firewall zone DMZ
[USG-zone-dmz]add interface GigabitEthernet 0/0/0
[USG-zone-dmz]quit
[USG]firewall zone untrust
[USG-zone-untrust]add interface GigabitEthernet 0/0/1
[USG-zone-untrust]quit
```

Step 4 配置域间包过滤策略。

```
[USG]policy interzone dmz untrust inbound
[USG-policy-interzone-dmz-untrust-inbound]policy 0
[USG-policy-interzone-dmz-untrust-inbound-0]policy destination 192.168.1.2
0.0.0.255
[USG-policy-interzone-dmz-untrust-inbound-0]policy service service-set ftp
[USG-policy-interzone-dmz-untrust-inbound-0]action permit
```

Step 5 配置 NAT server。

```
[USG] nat server protocol tcp global 2.2.2.1 ftp inside 192.168.1.2 ftp
```

Step 6 配置 NAT 地址池。

```
[USG] nat address-group 1 192.168.1.10 192.168.1.20
```

Step 7 在 DMZ 与 Untrust 域间应用 NAT ALG 功能,使服务器可以正常对外提供 FTP 服务。

```
[USG] firewall interzone dmz untrust
[USG-interzone-dmz-untrust] detect ftp
[USG-interzone-dmz-untrust] quit
```

Step 8 创建 DMZ 区域和 Untrust 区域之间的 NAT 策略，确定进行 NAT 转换的源地址范围，并且将其与 NAT 地址池 1 进行绑定。

```
[USG] nat-policy interzone dmz untrust inbound
[USG-nat-policy-interzone-dmz-untrust-inbound] policy 0
[USG-nat-policy-interzone-dmz-untrust-inbound-0] policy source 2.2.2.0
0.0.0.255
[USG-nat-policy-interzone-dmz-untrust-inbound-0] action source-nat
[USG-nat-policy-interzone-dmz-untrust-inbound-0] address-group 1
[USG-nat-policy-interzone-dmz-untrust-inbound-0] quit
[USG-nat-policy-interzone-dmz-untrust-inbound] quit
```



实验步骤 – Web

Step 1 设置 server 地址和 PC 地址。

Step 2 设置防火墙 GE0/0/0 和 GE0/0/1 的 IP 地址。选择“网络 > 接口 > 接口”。在“接口列表”中单击各接口对应的 。配置如下图所示：配置完成后单击“应用”。

接口名称	GigabitEthernet0/0/0 *	
别名		
VPN实例	public *	
安全区域	dmz	
模式	◉ 路由 ○ 交换	
连接类型	◉ 静态IP ○ DHCP ○ PPPoE	
IP地址	192 . 168 . 1 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

接口名称	GigabitEthernet0/0/1 *	
别名		
VPN实例	public *	
安全区域	untrust	
模式	◉ 路由 ○ 交换	
连接类型	◉ 静态IP ○ DHCP ○ PPPoE	
IP地址	2 . 2 . 2 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

Step 3 配置域间包过滤策略。选择“防火墙 > 安全策略 > 转发策略”。选择“转发策略”页签。在“转发策略列表”中单击 。配置如下图所示：配置完成后单击“应用”。

源安全区域	untrust *	
目的安全区域	dmz *	
源地址	any	多选
目的地址	any	多选
用户	any	多选
服务	ftp	多选
时间段	all	
动作	permit *	
描述		

Step 4 配置 NAT server。选择“防火墙 ＞NAT＞ 虚拟服务器”。在“虚拟服务器列表”中单击 ✚。配置如图所示：配置完成后单击“应用”。

防火墙 > NAT > 虚拟服务器

新建虚拟服务器

映射方式	一对一地址映射
外部地址	2.2.2.4 *
内部地址	192 . 168 . 1 . 2 *
端口转换	☑
协议	● TCP ○ UDP
外部端口	21(ftp)
内部端口	21(ftp)

应用 返回

Step 5 配置 NAT 地址池。选择“防火墙 ＞NAT＞ 源 NAT”。选择“NAT 地址池”页签。在“NAT 地址池列表”中单击 ✚，NAT 地址池的参数配置如图所示：

防火墙 > NAT > 源NAT

源NAT | NAT地址池

新建NAT地址池

地址池号 1 *<0-1023>

地址池名称

起始IP 192 . 168 . 1 . 10 *

结束IP 192 . 168 . 1 . 20 *

应用 返回

Step 6 配置源 NAT，选择“防火墙 ＞NAT＞ 源 NAT”，选择“源 NAT”页，在“源 NAT 策略列表”列表中单击 ，源 NAT 的参数配置如图所示

防火墙 > NAT > 源NAT

新建源NAT

源安全区域 untrust *

目的安全区域 dmz *

源地址 2.2.2.0\0.0.0.255 多选

目的地址 any 多选

动作 NAT转换 *

描述

将源地址转换为 地址池中的地址 接口IP地址

地址池 1 *

允许端口地址转换

验证结果

使用命令 display nat server 查看 NAT server 对应情况：

```
[USG]dis nat server
Server in private network information:
 id                 : 0
 zone                : ---
 interface          : ---
 global-start-addr : 2.2.2.4              global-end-addr    : ---
 inside-start-addr : 192.168.1.20          inside-end-addr    : ---
```

```
global-start-port : ---                global-end-port    : ---
insideport          : ---
globalvpn           : public             insidevpn          : public
protocol            : ---                vrrp               : ---
no-reverse          : no

 Total    1 NAT servers
```

5.3 双出口NAT实验(基于zone的NATserver+双出口)

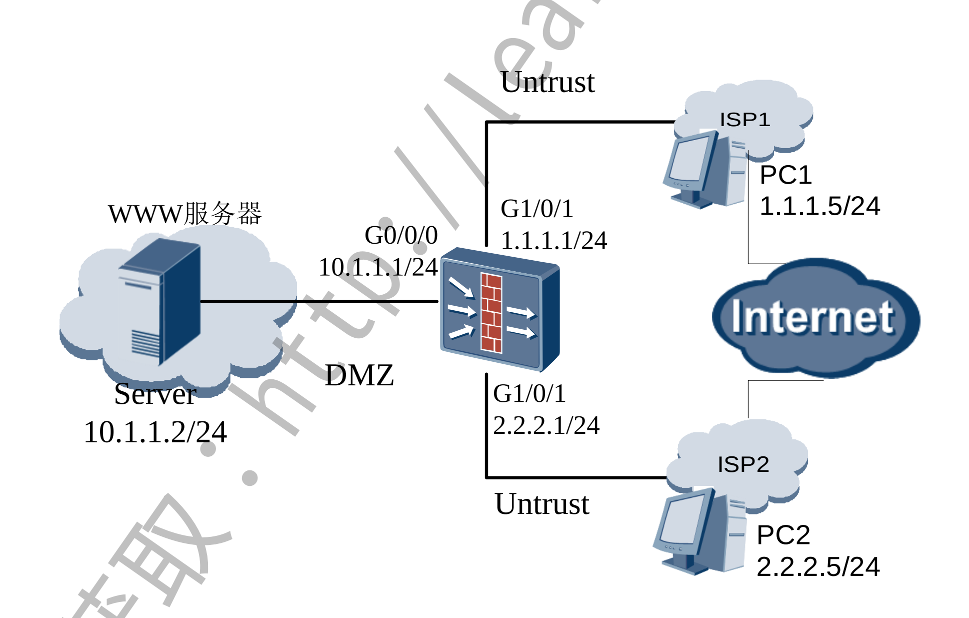
实验目的

学会配置双出口 NAT.学会配置基于 zone 的 NAT server。

组网设备

WWW server 一台，PC 机两台，USG 防火墙一台。

实验拓扑图



实验步骤 -CLI

Step 1 配置 PC1、PC2 和 WWW 服务器的 IP 地址。具体步骤省略。

Step 2 配置防火墙接口地址。

```
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0]ip address 10.1.1.1 255.255.255.0
```

```
[USG-GigabitEthernet0/0/0]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]ip address 1.1.1.1 255.255.255.0
[USG-GigabitEthernet0/0/1]quit
[USG]interface GigabitEthernet 0/0/2
[USG-GigabitEthernet0/0/2]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet0/0/2]quit
[USG]firewall zone dmz
[USG-zone-trust]add interface GigabitEthernet 0/0/0
[USG-zone-trust]quit
```

Step 3 创建两个新的安全区域并将 GE0/0/1 和 GE0/0/2 加入相应的安全区域。

```
[USG]firewall zone name ISP1
[USG-zone-isp1]set priority 10
[USG-zone-isp1]add int GigabitEthernet 0/0/1
[USG-zone-isp1]quit
[USG]firewall zone name ISP2
[USG-zone-isp2]set priority 15
[USG-zone-isp2]add int GigabitEthernet 0/0/2
[USG-zone-isp2]quit
```

Step 4 配置相应的域间包过滤策略。

```
[USG] policy interzone dmz isp1 inbound
[USG-policy-interzone-dmz-isp1-inbound] policy 0
[USG-policy-interzone-dmz-isp1-inbound-0] policy destination 10.1.1.2 0
[USG-policy-interzone-dmz-isp1-inbound-0] policy service service-set http
[USG-policy-interzone-dmz-isp1-inbound-0] action permit
[USG-policy-interzone-dmz-isp1-inbound-0] quit
[USG-policy-interzone-dmz-isp1-inbound] quit
[USG] policy interzone dmz isp2 inbound
[USG-policy-interzone-dmz-isp2-inbound] policy 0
[USG-policy-interzone-dmz-isp2-inbound-0] policy destination 10.1.1.2 0
[USG-policy-interzone-dmz-isp2-inbound-0] policy service service-set http
[USG-policy-interzone-dmz-isp2-inbound-0] action permit
[USG-policy-interzone-dmz-isp2-inbound-0] quit
[USG-policy-interzone-dmz-isp2-inbound] quit
```

Step 5 配置内部服务器，对不同的安全区域发布不同的公网 IP 地址。

```
[USG] nat server zone isp1 protocol tcp global 1.1.1.2 inside 10.1.1.2
[USG] nat server zone isp2 protocol tcp global 2.2.2.2 inside 10.1.1.2
```

实验步骤 - Web

Step 1 配置 PC1、PC2 和 WWW 服务器的 IP 地址。具体步骤省略。

Step 2 配置防火墙接口地址。 选择“网络 > 接口 > 接口”。在“接口列表”中单击各接口对应的 。具体步骤省略。

Step 3 创建两个新的安全区域并将 GE0/0/1 和 GE0/0/2 加入相应的安全区域。选择“网络 > 安全区域 > 安全区域”。单击“安全区域列表”中的“新建”。依次输入各项参数，如图所示：

网络 > 安全区域 > 安全区域

新建安全区域

安全区域名称	ISP1 *
优先级	10 *<1-100>
描述	

应用 返回

网络 > 安全区域 > 安全区域

新建安全区域

安全区域名称	ISP2 *
优先级	15 *<1-100>
描述	

应用 返回

Step 4 配置相应的域间包过滤策略。

源安全区域	isp1 *	
目的安全区域	dmz *	
源地址	请选择或输入IP地址	多选
目的地址	请选择或输入IP地址	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

源安全区域	isp2 *
目的安全区域	dmz *
源地址	请选择或输入IP地址 [多选]
目的地址	请选择或输入IP地址 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

Step 5 配置内部服务器，对不同的安全区域发布不同的公网 IP 地址。选择“防火墙 > NAT > 虚拟服务器”。在“虚拟服务器列表”中单击 新建。创建到两个出口的虚拟服务器映射。

映射方式	一对一地址映射
外部地址	1.1.1.2 *
内部地址	10 . 1 . 1 . 2 *
端口转换	☐
	[应用] [返回]

映射方式	一对一地址映射
外部地址	2.2.2.1 *
内部地址	10 . 1 . 1 . 2 *
端口转换	☐
	[应用] [返回]

验证结果

查看 NAT Server.

```
[USG]display nat server
Server in private network information:
 id                    : 0
 zone                   : isp1
 interface             : ---
```

```
global-start-addr : 1.1.1.1           global-end-addr    : ---
inside-start-addr : 10.1.1.2          inside-end-addr    : ---
global-start-port : 0(any)            global-end-port    : ---
insideport          : 0(any)
globalvpn           : public             insidevpn          : public
protocol            : tcp                vrrp               : ---
no-reverse          : no

id                  : 1
zone                : isp2
interface           : ---
global-start-addr : 2.2.2.1           global-end-addr    : ---
inside-start-addr : 10.1.1.2          inside-end-addr    : ---
global-start-port : 0(any)            global-end-port    : ---
insideport          : 0(any)
globalvpn           : public             insidevpn          : public
protocol            : tcp                vrrp               : ---
no-reverse          : no
Total     2 NAT servers
```

使用 display firewall session table 查看 nat server 转换情况：

```
[USG]dis firewall session table
09:29:38   2013/05/22
 Current Total Sessions : 11
  icmp   VPN:public --> public 10.1.1.1:52651-->10.1.1.2:2048
  icmp   VPN:public --> public 1.1.1.1:52907-->1.1.1.2:2048
  icmp   VPN:public --> public 2.2.2.1:53163-->2.2.2.2:2048
  icmp   VPN:public --> public 2.2.2.2:256-->10.1.1.2:2048
  icmp   VPN:public --> public 1.1.1.2:256-->10.1.1.2:2048
  http   VPN:public --> public 1.1.1.2:2053-->10.1.1.2:80
  http   VPN:public --> public 2.2.2.2:2050-->10.1.1.2:80
  http   VPN:public --> public 2.2.2.2:2051-->10.1.1.2:80
  http   VPN:public --> public 2.2.2.2:2052-->10.1.1.2:80
  http   VPN:public --> public 2.2.2.2:2053-->10.1.1.2:80
  http   VPN:public --> public 1.1.1.2:2054-->10.1.1.2:80
```

6 防火墙双机热备实验

6.1 防火墙双机热备实验

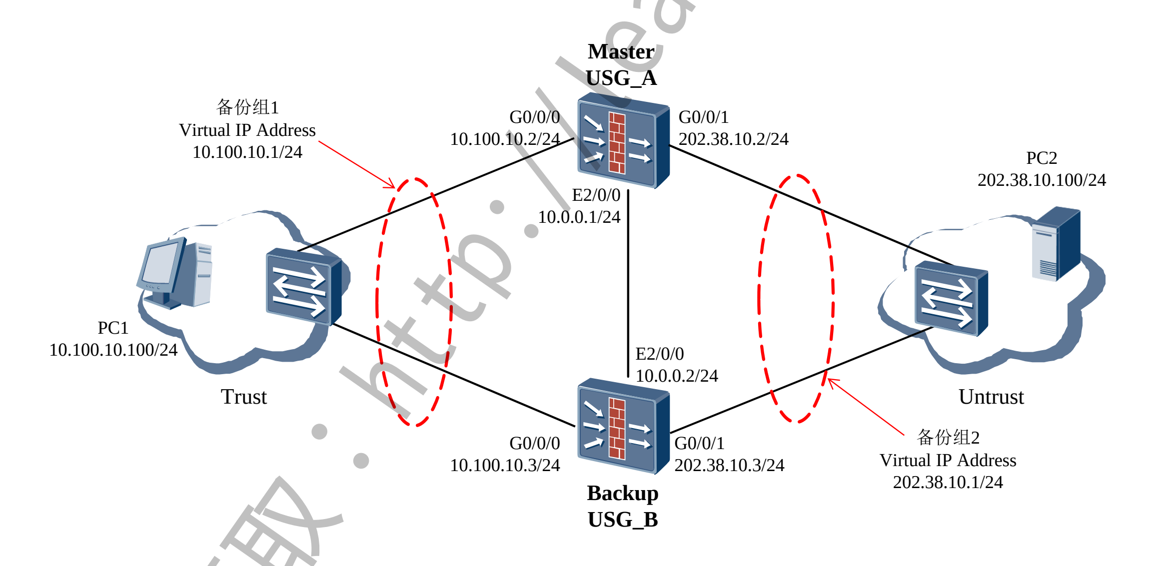
实验目的

熟悉通过命令行和 web 方式配置防火墙双机热备，USG 作为安全设备被部署在业务节点上。其中上下行设备均是交换机，USG_A、USG_B 以主备备份方式工作，且上下行业务接口工作在三层。

组网设备

1. 两台同型号的 USG2200 或两台同型号的 USG5000 防火墙，2 台交换机，两台 PC
2. 防火墙至少有三个业务接口

实验拓扑图



实验步骤 - CLI

Step 1 完成 USG_A 上、下行业务接口的配置。配置各接口 IP 地址并加入相应安全区域。

```
<USG_A> system-view
[USG_A] interface GigabitEthernet 0/0/0
[USG_A-GigabitEthernet0/0/0] ip address 10.100.10.2 24
[USG_A-GigabitEthernet0/0/0] quit
[USG_A] interface GigabitEthernet 0/0/1
```

```
[USG_A-GigabitEthernet0/0/3] ip address 202.38.10.2 24
[USG_A-GigabitEthernet0/0/3] quit
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface GigabitEthernet 0/0/0
[USG_A-zone-trust] quit
[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface GigabitEthernet 0/0/1
[USG_A-zone-untrust] quit
```

配置接口 GigabitEthernet 0/0/0 的 VRRP 备份组 1，并加入到状态为 Master 的 VGMP 管理组。

```
[USG_A] interface GigabitEthernet 0/0/0
[USG_A-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.100.10.1 master
[USG_A-GigabitEthernet0/0/1] quit
```

配置接口 GigabitEthernet 0/0/1 的 VRRP 备份组 2，并加入到状态为 Master 的 VGMP 管理组。

```
[USG_A] interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/3] vrrp vrid 2 virtual-ip 202.38.10.1 master

[USG_A-GigabitEthernet0/0/3] quit
```

Step 2 配置域间过滤保证通讯

```
[USG] firewall packet-filter default permit interzone trust untrust
```

Step 3 完成 USG_A 的心跳线配置。

配置 Ethernet2/0/0 的 IP 地址。

```
[USG_A] interface Ethernet2/0/0
[USG_A-GigabitEthernet0/0/2] ip address 10.0.0.1 24
[USG_A-GigabitEthernet0/0/2] quit
```

配置 Ethernet2/0/0 加入 DMZ 区域。

```
[USG_A] firewall zone dmz
[USG_A-zone-dmz] add interface Ethernet2/0/0
[USG_A-zone-dmz] quit
```

指定 Ethernet2/0/0 为心跳口。

```
[USG_A] hrp interface Ethernet2/0/0
```

Step 4 启用 HRP 备份功能。

```
[USG_A] hrp enable
```

Step 5 配置 Trust 区域和 Untrust 区域的域间转发策略。

配置 Trust 区域和 Untrust 区域的域间转发策略。

```
HRP_M[USG_A] policy interzone trust untrust outbound
HRP_M[USG_A-policy-interzone-trust-untrust-outbound] policy 1
```

```
HRP_M[USG_A-policy-interzone-trust-untrust-outbound-1] policy source 10.100.10.0 0.0.0.255
HRP_M[USG_A-policy-interzone-trust-untrust-outbound-1] action permit
HRP_M[USG_A-policy-interzone-trust-untrust-outbound-1] quit

HRP_M[USG_A-policy-interzone-trust-untrust-outbound] quit
```

Step 6 配置 USG_B。

USG_B 和上述 USG_A 的配置基本相同，不同之处在于：

1. USG_B 各接口的 IP 地址与 USG_A 各接口的 IP 地址不相同。
2. USG_B 的业务接口 GigabitEthernet0/0/0 和 GigabitEthernet0/0/1 加入状态为 Slave 的 VGMP 管理组。

Step 7 配置 Switch。

分别将两台 Switch 的三个接口加入同一个 VLAN，具体配置命令请参考交换机的相关文档。

Step 8 配置静态路由。

在内网中的 PC 上配置静态路由，将 VRRP 备份组的虚拟 IP 地址作为到达其他网段的下一跳地址。

实验步骤 – Web

Step 1 完成 USG_A 防火墙接口配置。选择“网络 > 接口 > 接口”。 单击需要配置接口后面的配置按钮 。 依次选择或输入各项参数 单击“应用”。 配置完成后如下图所示。



Step 2 完成 USG_A 防火墙域间转发策略配置。

Trust 与 untrust 间转发策略：选择“防火墙 > 安全策略 > 转发策略”。 在“转发策略列表”中，单击“新建”。 依次输入或选择各项参数。 单击“应用”。

完成 Trust 与 untrust 间转发策略如图所示。



防火墙 DMZ 本地策略：选择“防火墙 > 安全策略 > 本地策略”。 在“对设备访问控制列表”中，选择默认策略，动作改为 permit ，单击“应用”。

完成防火墙 DMZ 本地策略配置如图。



Step 3 完成 USG_A 防火墙 VRRP 备份组 1 和 VRRP 备份组 2 的配置

新建 VRRP 备份组 1。选择“系统 > 高可靠性 > 双机热备”。 在“VRID 列表”中，单击“新建”。 依次输入或选择各项参数。单击“应用”。

系统 > 高可靠性 > 双机热备

新建VRID

VRRP VRID 1 *<1-255>

接口名称 GE0/0/0 * 查看配置

接口IP地址/掩码 10.100.10.2 * 255.255.255.0

虚IP地址/掩码 10.100.10.1 * 255.255.255.0

管理组 Active Standby

高级

应用 返回

同上操作新建 VRRP 备份组 2

系统 > 高可靠性 > 双机热备

新建VRID

VRRP VRID 2 *<1-255>

接口名称 GE0/0/1 * 查看配置

接口IP地址/掩码 202.38.10.2 * 255.255.255.0

虚IP地址/掩码 202.38.10.1 * 255.255.255.0

管理组 Active Standby

高级

应用 返回

Step 4 完成 USG_A 防火墙 HRP 配置。选择“系统 > 高可靠性 > 双机热备”。 选中“HRP 启动”。 选择 HRP 备份通道的接口 FE2/0/0。点击高级进入高级选项，依次输入或选择各项参数。单击“应用”。



USG_B 防火墙配置与 USG_A 防火墙基本一致，略。

实验结果

在 USG_A 上执行 **display vrrp** 命令，检查 VRRP 组内接口的状态信息，显示以下信息表示 VRRP 组建立成功。

```
HRP_M<USG_A>dis vrrp
16:12:02   2013/06/08
  GigabitEthernet0/0/1 | Virtual Router 2
    VRRP Group : Master
    state : Master
    Virtual IP : 202.38.10.1
    Virtual MAC : 0000-5e00-0102
    Primary IP : 202.38.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES     Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  GigabitEthernet0/0/0 | Virtual Router 1
    VRRP Group : Master
    state : Master
    Virtual IP : 10.100.10.1
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.100.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES     Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

在 USG_A 上执行 display hrp state 命令，检查当前 HRP 的状态，显示以下信息表示 HRP 建立成功。

```
HRP_M<USG_A>dis hrp state
16:15:31   2013/06/08
 The firewall's config state is: MASTER

 Current state of virtual routers configured as master:
             GigabitEthernet0/0/1     vrid     2 : master
```

```
            GigabitEthernet0/0/0       vrid      1 : master
```

在处于 Trust 区域的 PC1 端 ping VRRP 组 1 的虚拟 IP 地址 10.100.10.1，在 USG_A 上检查会话。

```
HRP_M<USG_A>display firewall session table
16:17:36    2013/06/08
 Current Total Sessions : 1
  icmp    VPN:public --> public 10.100.10.100:1-->10.100.10.1:2048
```

可以看出 VRRP 组配置正确后，在 PC1 端能够 ping 通 VRRP 组 1 的虚拟 IP 地址。

PC2 作为服务器位于 Untrust 区域。在 Trust 区域的 PC1 端能够 ping 通 Untrust 区域的服务器。分别在 USG_A 和 USG_B 上检查会话。

```
HRP_M<USG_A>display firewall session table
16:19:42    2013/06/08
 Current Total Sessions : 1
  icmp    VPN:public --> public 10.100.10.100:1-->202.38.10.100:2048

HRP_S<USG_B>display firewall session table
16:03:19    2013/06/08
 Current Total Sessions : 1
  icmp    VPN:public --> public    Remote 10.100.10.100:1-->202.38.10.100:2048
```

可以看出 USG_B 上存在带有 Remote 标记的会话，表示配置双机热备功能后，会话备份成功。

在 PC1 上执行 ping 202.38.10.100 –t ，然后将 USG_A 防火墙 G0/0/0 接口网线拔出，观察防火墙状态切换及 ping 包丢包情况；再将 USG_A 防火墙 G0/0/0 接口网线恢复，观察防火墙状态切换及 ping 包丢包情况。

7 防火墙用户管理

7.1 上网用户认证（免认证和密码认证）

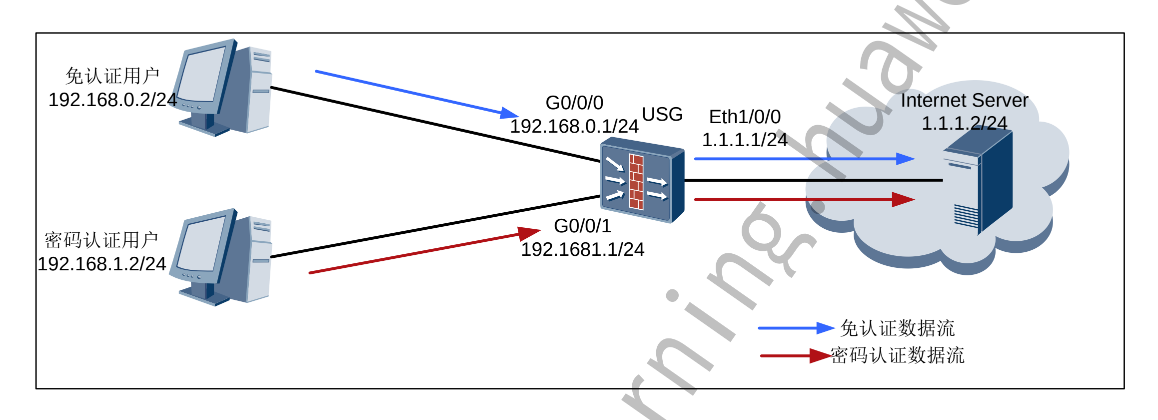
实验目的

介绍免认证和密码认证的应用场景和配置方法。

组网设备

USG 防火墙一台，PC 机一台。

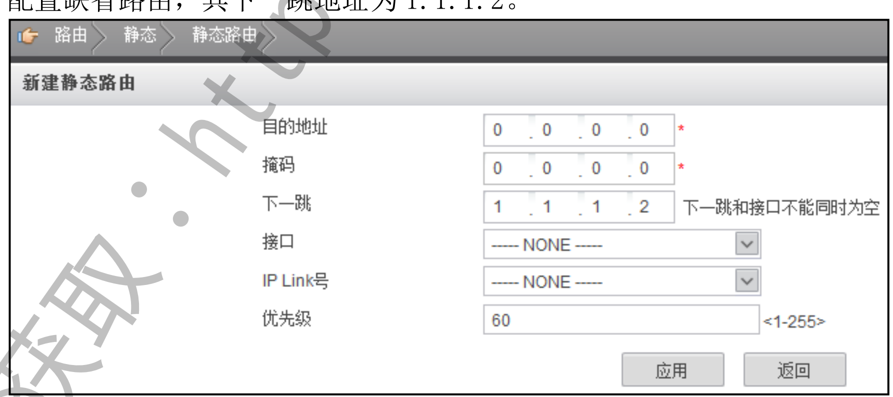
实验拓扑图



实验步骤（Web）

Step 6 配置 USG 的接口基本参数，并加入安全域。G0/0/0 加入 guest 区域，G0/0/1 加入 Trust，Eth1/0/0 加入 Untrust。具体步骤略。

Step 7 配置缺省路由，其下一跳地址为 1.1.1.2。



Step 8 创建免认证用户组。

选择“用户 > 上网用户 > 组/用户”。

在“组织结构”中，选择“root”。

在“成员管理”中单击“新建”，选择“新建组”，组名 guest。

用户 > 上网用户 > 组/用户

组织结构

查询

root

免认证

组成员

组路径： root[配置]

描述：

组信息： 子组个数：1 直属用户个数：

成员管理

新建 删除 刷新 批量修改 移动 导出

新建用户

新建多用户

新建组

添加已有用户

所属组

root

修改用户组

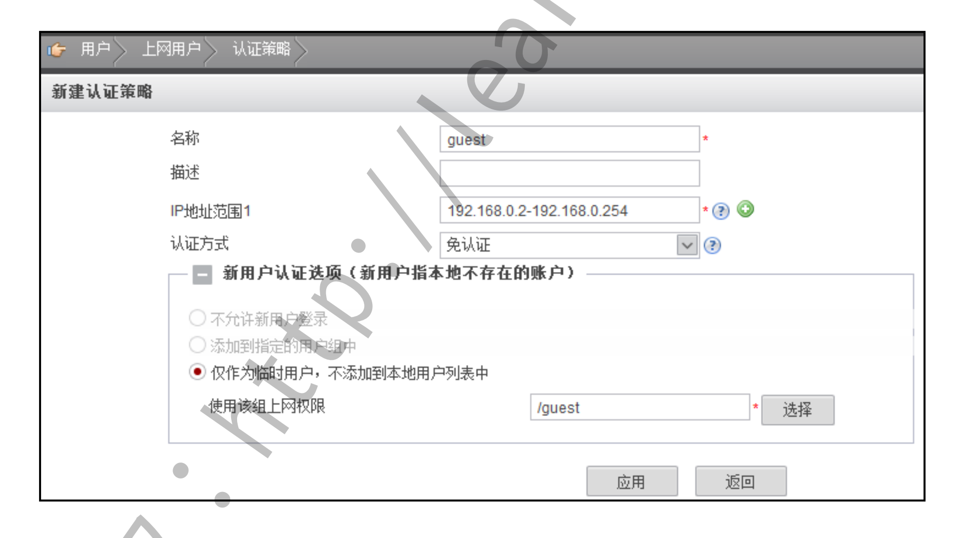
组名 guest *

描述

所属组 root 选择

应用 返回

Step 9 创建网段 192.168.0.0/24 对应的用户认证策略 guest。



Step 10 创建密码认证用户组和用户。

选择“用户 > 上网用户 > 组/用户”。

在“组织结构”中，选择“root”。

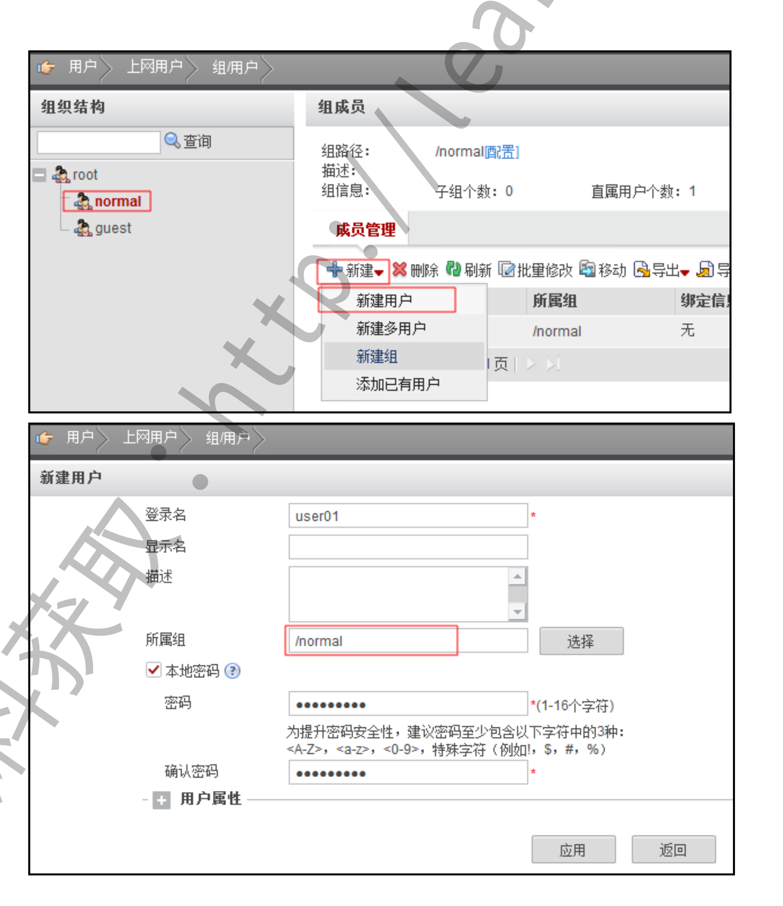
在“成员管理”中单击“新建”，选择“新建组”，组名 Normal。





在“组织结构”中，选择“normal”。

在“成员管理”中单击“新建”，选择“新建用户”，用户名 user01 密码 Admin@123。



Step 11 创建网段 192.168.1.0/24 对应的用户认证策略 normal。

用户 > 上网用户 > 认证策略

新建认证策略

名称 normal *
描述
IP地址范围1 192.168.1.2-192.168.1.254 *
认证方式 本地密码认证/服务器认证
认证服务器类型 RADIUS LDAP AD
认证服务器名称 ---- NONE ----
新用户认证选项（新用户指本地不存在的账户）
应用 返回

Step 12 为免认证用户创建转发策略。选择源安全区域 guest，目的安全区域为 untrust，并选择免认证用户组 guest，动作为 Permit。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域 guest *
目的安全区域 untrust *
源地址 请选择或输入IP地址 多选
目的地址 any 多选
用户 /guest 多选
服务 请选择服务 多选
时间段 all
动作 permit *
描述

Step 13 为密码认证用户创建转发策略。

选择源安全区域 trust，目的安全区域为 untrust，并选择密码认证用户组 normal，动作为 Permit。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域 trust *
目的安全区域 untrust *
源地址 请选择或输入IP地址 多选
目的地址 any 多选
用户 /normal 多选
服务 请选择服务 多选
时间段 all
动作 permit *
描述

网络 > 接口 > 接口

修改GigabitEthernet

接口名称 GigabitEthernet0/0/0 *
别名
VPN实例 public *
安全区域 trust
模式 路由 交换
连接类型 静态IP DHCP PPPoE
IP地址 192 . 168 . 5 . 1
子网掩码 255 . 255 . 255 . 0
默认网关

Step 14 配置上网认证推送页面配置，设置重定向方式是 HTTP，并设置认证端口是 8888。



当用户通过 Http 方式访问 Internet 的业务，将重定向到上网用户认证页面。

思考：重定向认证方式 HTTP 和 HTTPS 的区别。

验证结果

临时用户不需要输入用户名密码，即可以访问 Internet。

普通员工通过 HTTP 访问 Internet 时，USG 应推送用户认证页面，提示用户输入用户名和密码。用户只有输入正确的用户名和密码后，才能访问网络资源。

8 防火墙互联技术实验

8.1 VLAN 实验（配置 VLAN 间通过 Vlanif 接口通信）

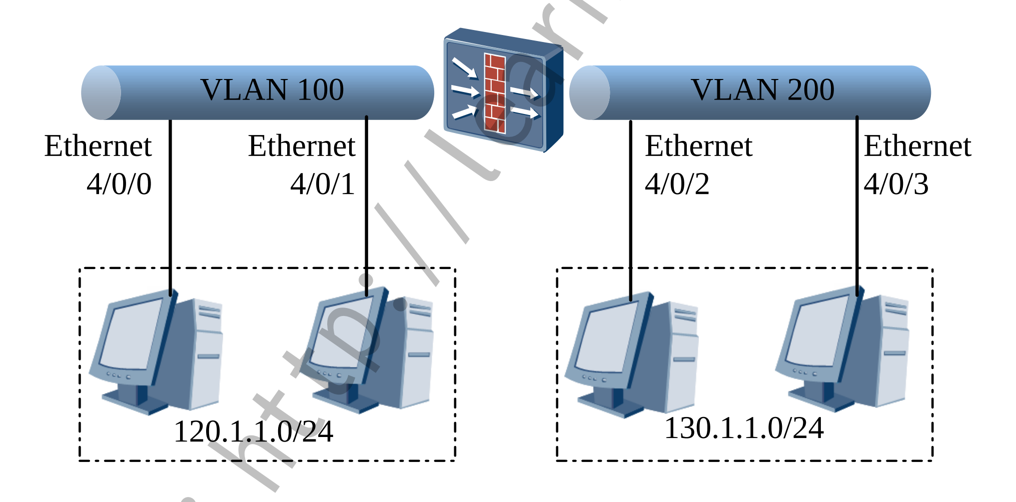
实验目的

通过本实验，你将学会如何配置 VLAN 间通过 Vlanif 接口通信。

组网设备

USG 防火墙一台，PC 机四台。

实验拓扑图



实验步骤

Step 1 配置 VLAN，并加入接口。

创建 VLAN100。

```
<USG> system-view
[USG] vlan 100
[USG-vlan-100] quit
```

在 VLAN100 中加入端口 Ethernet 4/0/0。

```
[USG] interface Ethernet 4/0/0
[USG-Ethernet4/0/0] port access vlan 100
[USG-Ethernet4/0/0] quit
```

在 VLAN100 中加入端口 Ethernet 4/0/1。

```
[USG] interface Ethernet 4/0/1
[USG-Ethernet4/0/1] port access vlan 100
[USG-Ethernet4/0/1] quit
```

创建 VLAN200。

```
[USG] vlan 200
[USG-vlan-200] quit
```

在 VLAN200 中加入端口 Ethernet 4/0/2。

```
[USG] interface Ethernet 4/0/2
[USG-Ethernet4/0/2] port access vlan 200
[USG-Ethernet4/0/2] quit
```

在 VLAN200 中加入端口 Ethernet 4/0/3。

```
[USG] interface Ethernet 4/0/3
[USG-Ethernet4/0/3] port access vlan 200
[USG-Ethernet4/0/3] quit
```

Step 2 配置 Vlanif 接口。

配置 Vlanif100 的 IP 地址。

```
[USG] interface vlanif 100
[USG-Vlanif100] ip address 120.1.1.1 24
[USG-Vlanif100] quit
```

配置 Vlanif200 的 IP 地址。

```
[USG] interface vlanif 200
[USG-Vlanif200] ip address 130.1.1.1 24
[USG-Vlanif200] quit
```

Step 3 将接口加入安全区域，并配置域间包过滤，以保证网络基本通信正常。

```
[USG]firewall zone trust
[USG-zone-trust]add interface Vlanif 100
[USG-zone-trust]quit
[USG]firewall zone untrust
[USG-zone-untrust] add interface Vlanif 200
[USG-zone-untrust] quit
[USG] policy interzone trust untrust inbound
[USG-policy-interzone-trust-untrust-inbound] policy 0
[USG-policy-interzone-trust-untrust-inbound-0] action permit
[USG-policy-interzone-trust-untrust-inbound-0] quit
[USG-policy-interzone-trust-untrust-inbound] quit
[USG] policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound] policy 0
[USG-policy-interzone-trust-untrust-outbound-0] action permit
[USG-policy-interzone-trust-untrust-outbound-0] quit
```

```
[USG-policy-interzone-trust-untrust-outbound] quit
```

Step 4 配置属于 VLAN100 的主机网关为 120.1.1.1，配置属于 VLAN200 的主机网关为 130.1.1.1。在主机上设置，具体步骤省略。

验证结果

配置完成后，属于 VLAN100 和 VLAN200 的主机之间可以相互 ping 通：

```
PC2>ping 120.1.1.2

Ping 120.1.1.2: 32 data bytes, Press Ctrl_C to break
From 120.1.1.2: bytes=32 seq=1 ttl=127 time=47 ms
From 120.1.1.2: bytes=32 seq=2 ttl=127 time=31 ms
From 120.1.1.2: bytes=32 seq=3 ttl=127 time=47 ms
From 120.1.1.2: bytes=32 seq=4 ttl=127 time=31 ms
From 120.1.1.2: bytes=32 seq=5 ttl=127 time=47 ms

--- 120.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/40/47 ms

PC1>ping 130.1.1.2

Ping 130.1.1.2: 32 data bytes, Press Ctrl_C to break
From 130.1.1.2: bytes=32 seq=1 ttl=127 time=16 ms
From 130.1.1.2: bytes=32 seq=2 ttl=127 time=31 ms
From 130.1.1.2: bytes=32 seq=3 ttl=127 time=31 ms
From 130.1.1.2: bytes=32 seq=4 ttl=127 time=31 ms
From 130.1.1.2: bytes=32 seq=5 ttl=127 time=47 ms

--- 130.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 16/31/47 ms
```

8.2 WLAN 实验（Crypto 服务类）

实验目的

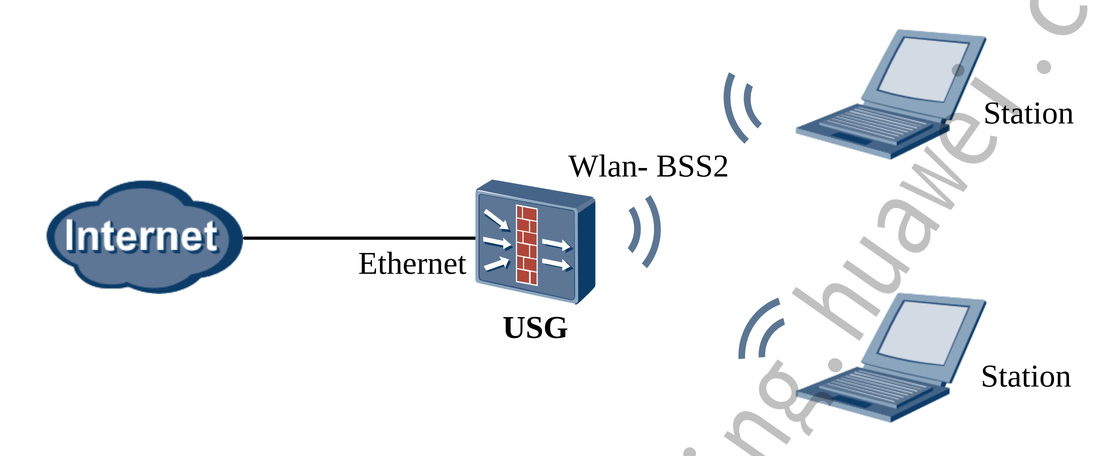
通过本实验，你将学会在新建无线服务后，无线用户可以搜索到无线服务的网络名称

（SSID）并连接到无线局域网。

组网设备

带有无线网卡的主机一台，USG2110-X 防火墙 1 台

实验拓扑图



实验步骤

Step 1 配置 GigabitEthernet 0/0/1 接口，将接口加入安全区域。

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip address 202.169.10.1 24
[USG-GigabitEthernet0/0/1] quit
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet 0/0/1
[USG-zone-untrust] quit
```

Step 2 创建 VLAN 及对应 Vlanif 接口，将 Vlanif 接口加入安全区域。

```
[USG] vlan 2
[USG-vlan-2] quit
[USG] interface Vlanif 2
[USG-Vlanif2] ip address 192.168.1.1 255.255.255.0
[USG-Vlanif2] quit
[USG] firewall zone trust
[USG-zone-trust] add interface Vlanif 2
[USG-zone-trust] quit
```

Step 3 配置 WLAN-BSS 接口。

创建 WLAN-BSS 接口。

```
[USG] interface wlan-bss 2
```

将 WLAN-BSS 接口加入到 VLAN2。

```
[USG-Wlan-Bss2] port access vlan 2
[USG-Wlan-Bss2] quit
```

Step 4 配置服务类。

创建服务类。

```
[USG] wlan service-class 2 crypto
```

配置 SSID。

```
[USG-wlan-sc-2] ssid WLAN100
```

配置认证模式。

```
[USG-wlan-sc-2] authentication-method wpa2-psk
```

配置数据帧的加密套件。

```
[USG-wlan-sc-2] encryption-suite ccmp
```

配置预共享（PSK）密钥。

```
[USG-wlan-sc-2] pre-shared-key pass-phrase abcdefgh
```

启用服务类。

```
[USG-wlan-sc-2] service-class enable
[USG-wlan-sc-2] quit
```

Step 5 配置射频接口。

设置射频接口使用的射频类型为 dot11gn。

```
[USG] interface Wlan-rf 4/0/0
[USG-Wlan-rf4/0/0] shutdown
[USG-Wlan-rf4/0/0] radio-type dot11gn
[USG-Wlan-rf4/0/0] undo shutdown
```

配置服务类与 WLAN-BSS 接口绑定。

```
[USG-Wlan-rf4/0/0] bind service-class 2 interface wlan-bss 2
[USG-Wlan-rf4/0/0] quit
```

Step 6 配置域间包过滤策略，保证网络正常通信。

打开 Trust 区域和 Untrust 区域之间的包过滤。

```
[USG] policy interzone trust untrust inbound
[USG-policy-interzone-trust-untrust-inbound] policy 0
[USG-policy-interzone-trust-untrust-inbound-0] action permit
[USG-policy-interzone-trust-untrust-inbound-0] quit
[USG-policy-interzone-trust-untrust-inbound] quit
```

为实现 Station 和 AP 互相访问，需要打开 Station 所在安全区域和 Local 安全区域之间的包过滤。

```
[USG] policy interzone trust local inbound
[USG-policy-interzone-local-trust-inbound] policy 0
[USG-policy-interzone-local-trust-inbound-0] action permit
[USG-policy-interzone-local-trust-inbound-0] quit
```

```
[USG-policy-interzone-local-trust-inbound] quit
[USG] policy interzone trust local outbound
[USG-policy-interzone-local-trust-outbound] policy 0
[USG-policy-interzone-local-trust-outbound-0] action permit
[USG-policy-interzone-local-trust-outbound-0] quit
[USG-policy-interzone-local-trust-outbound] quit
```

Step 7 配置缺省路由。

```
[USG] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

Step 8 配置客户端无线网卡（客户端的操作系统以 Windows XP 为例）。

静态配置无线网卡 IP 地址：192.168.1.2/24 和 192.168.1.3/24。

a) 选择“开始 > 控制面板 > 网络连接”，在“网络连接”中选择“本地连接”。
b) 在弹出界面的“常规”页签中选择“属性”。
c) 在弹出界面的“常规”页签中选择“Internet 协议（TCP/IP）”。
d) 在弹出界面的“常规”页签中选择“使用下面的 IP 地址”，在“IP 地址”框中输入 IP 地址（分别为 192.168.1.2、192.168.1.3），在“子网掩码”框中输入子网掩码（255.255.255.0），在“默认网关”中输入网关地址（输入 Vlanif 2 的 IP 地址 192.168.1.1）。

配置无线网卡上的 SSID、加密方式、认证模式、预共享（PSK）密钥，注意与 USG 设备上保持一致。

e) 选择“开始 > 控制面板 > 网络连接”，在“网络连接”中右键单击“无线网络连接”，选择“属性”。
f) 在弹出界面的“无线网络配置”页签中勾选“用 Windows 配置我的无线网络设置”，单击确认。
g) 选择“开始 > 控制面板 > 网络连接”，在“网络连接”中右键单击“无线网络连接”，选择“属性”。
h) 在弹出界面的“无线网络配置”页签中选择“添加”。
i) 在弹出界面的“关联”页签中，取消勾选“自动为我提供此密钥”，在“网络名（SSID）”中输入 SSID，在“无线网络密钥”中的“网络身份验证”下拉菜单中选择认证方式，在“数据加密”下拉菜单中选择加密方式，在“网络密钥”输入框中输入密钥，并在“确认网络密钥”中重复输入密钥进行确认，单击“确定”。
j) 在弹出界面的“无线网络配置”页签中选择“查看无线网络”。
k) 在弹出界面的“无线网络连接”页签中的右侧列举了无线工作站搜索到的 AP 信息，选择对应 SSID，双击进行连接。

验证结果

无线客户端可以 ping 通 USG 防火墙接口地址。

8.3 E1 实验

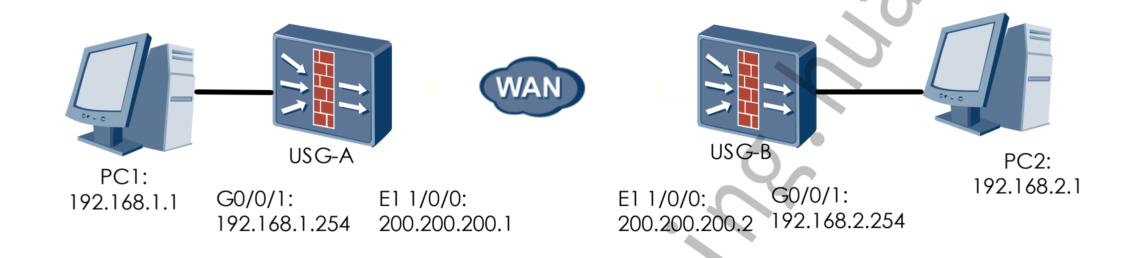
实验目的

为模拟广域网，在 USG 防火墙上安装 E1 接口卡，分别通过 WEB 和 CLI 这两种方式实现设备间互通；

组网设备

两台 USG2200，两台 PC，E1 线缆一根，网线两根。

实验拓扑图



实验步骤 – CLI

Step 1 配置 E1 1/0/0 接口的工作模式为 E1 模式。

```
<USG-A>system-view
[USG-A]controller E1 1/0/0
[USG-A-E1 1/0/0]using e1
[USG-A-E1 1/0/0]quit
<USG-B>system-view
[USG-B]controller E1 1/0/0
[USG-B-E1 1/0/0]using e1
[USG-B-E1 1/0/0]quit
```

Step 2 配置 Serial1/0/0:0 接口的 IP 地址。

```
[USG-A]interface Serial1/0/0:0
[USG-A-Serial1/0/0:0]ip address 200.200.200.1 255.255.255.0
[USG-A-Serial1/0/0:0]quit
[USG-B]interface Serial1/0/0:0
[USG-B-Serial1/0/0:0]ip address 200.200.200.2 255.255.255.0
[USG-B-Serial1/0/0:0]quit
```

Step 3 将 Serial1/0/0:0 接口加入 Untrust 安全区域。

```
[USG-A]firewall zone untrust
[USG-A-zone-untrust]add interface Serial1/0/0:0
```

```
[USG-A-zone-untrust]quit
[USG-B]firewall zone untrust
[USG-B-zone-untrust]add interface Serial1/0/0:0
[USG-B-zone-untrust]quit
```

Step 4 配置 GigabitEthernet 0/0/1 接口的 IP 地址。

```
[USG-A]interface GigabitEthernet 0/0/1
[USG-A-GigabitEthernet0/0/1]ip address 192.168.1.254 255.255.255.0
[USG-A-GigabitEthernet0/0/1]description to PC1
[USG-A-GigabitEthernet0/0/1]quit
[USG-B]interface GigabitEthernet 0/0/1
[USG-B-GigabitEthernet0/0/1]ip address 192.168.2.254 255.255.255.0
[USG-B-GigabitEthernet0/0/1]description to PC2
[USG-B-GigabitEthernet0/0/1]quit
```

Step 5 接口 GigabitEthernet 0/0/1 加入 Trust 安全区域。

```
[USG-A]firewall zone trust
[USG-A-zone-trust]add interface GigabitEthernet 0/0/1
[USG-A-zone-trust]quit
[USG-B]firewall zone trust
[USG-B-zone-trust]add interface GigabitEthernet 0/0/1
[USG-B-zone-trust]quit
```

Step 6 配置域间缺省包过滤。

```
[USG-A]firewall packet-filter default permit all
[USG-B]firewall packet-filter default permit all
```

Step 7 配置缺省路由。

```
[USG-A]ip route-static 0.0.0.0 0.0.0.0 200.200.200.2
[USG-B]ip route-static 0.0.0.0 0.0.0.0 200.200.200.1
```

实验步骤 – Web

Step 1 配置 USG-A 的接口（1）E1 1/0/0。选择“网络 > 接口 > 接口”。 在“接口列表”中单击 E1 4/0/0 所在行的 ，依次输入或选择各项参数，具体参数配置如下：

网络 > 接口 > 接口

修改E1

接口名称 E1 1/0/0 *
别名
当前E1模式 非成帧 成帧
线路编解码格式 AMI HDB3
帧格式 CRC4 NO-CRC4
时钟模式 主时钟 从时钟
时隙捆绑 时隙捆绑配置
时隙捆绑结果

应用 返回

Step 2 单击“时隙捆绑配置”；选择捆绑模式为“全部捆绑为一个 Serial 口”；单击“添加”；其他均为缺省值，单击“应用”。

时隙捆绑配置

捆绑模式 全部捆绑为一个Serial口 自定义捆绑
捆绑接口索引 *<0-30>
时隙范围 *<1-31,例子1,3,5-10>
添加 清空
时隙捆绑结果 0:1-31

确定 取消

配置 E1 1/0/0 后，“接口列表”上会显示新生成的接口 Serial 1/0/0:0，该接口为三层接口。



网络 > 接口 > 接口

接口列表

新建 删除 刷新 请选择查询类别 查询

接口名称	安全区域	IP地址	VLAN Tag	模式	连接类型	状态(物理/协...	启用	配置
E1 1/0/0								
Serial1/0/0:0	-NONE-(public)			Route	PPP			
FE2/0/0	-NONE-(public)			Route	IP			
GE0/0/0	trust(public)	192.168.17.3		Route	IP			
GE0/0/1	-NONE-(public)			Route	IP			
Serial4/0/0	-NONE-(public)			Route	PPP			

第 1 页共 1 页 显示 1 - 6，共 6 条

Step 3 配置接口 Serial1/0/0:0 加入到 Untrust 域，配置 GigabitEthernet0/0/1 接口加入到安全区域 Trust 域。选择“网络 > 接口 > 接口”，在“接口列表”中单击 Serial 1/0/0:0 所在行的编辑，依次输入或选择各项参数，具体参数配置如下：

接口名称	Serial1/0/0:0 *		
别名			
VPN实例	public *		
安全区域	untrust		
链路层协议	◉ PPP	○ HDLC	
类型	◉ 无	○ 客户端	○ 服务器
IP地址	200 . 200 . 200 . 1		
子网掩码	255 . 255 . 255 . 0		
NAT功能	☐ 启用		
☐ 启用访问管理	☐ HTTP	☐ HTTPS	☐ Ping
	☐ SSH	☐ SNMP	☐ Telnet

\+ 高级

修改GigabitEthernet

接口名称	GigabitEthernet0/0/1 *		
别名			
VPN实例	public *		
安全区域	trust		
模式	◉ 路由	○ 交换	
连接类型	◉ 静态IP	○ DHCP	○ PPPoE
IP地址	192 . 168 . 1 . 254	IP地址详细配置	
子网掩码	255 . 255 . 255 . 0		
默认网关	. . .		
NAT功能	☐ 启用		
☐ 启用访问管理	☐ HTTP	☐ HTTPS	☐ Ping
	☐ SSH	☐ SNMP	☐ Telnet

其他均为缺省值，单击“应用”。

Step 4 配置 USG-B（操作与 USG-A 相同，此处略。）

Step 5 USG-A 和 USG-B 上配置域间包过滤策略，以保证网络基本通信正常。 选择“防火墙 > 安全策略 > 转发策略”。 单击“untrust->trust”下的“默认”所在行的。 选择“动作”为“permit”。 单击“应用”。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	untrust *
目的安全区域	trust *
源地址	请选择或输入IP地址 [多选]
目的地址	请选择或输入IP地址 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

单击“trust->untrust”下的“默认”所在行的。 选择“动作”为“permit”。 单击“应用”。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	trust *
目的安全区域	untrust *
源地址	请选择或输入IP地址 [多选]
目的地址	请选择或输入IP地址 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

Step 6 USG-A 和 USG-B 上路由配置，以保证网络基本通信正常。选择“路由 > 策略路由 > 策略路由”， 单击“新建”；依次选择或输入各项参数，单击“应用”。

USG-A 静态路由配置

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	200 . 200 . 200 . 2 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

USG-B 静态路由配置

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	200 . 200 . 200 . 1 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

验证结果

从 USG-A 上使用源地址 192.168.1.1 Ping 192.168.2.2，结果应成功；

在 USG-A 上，选择“系统 > 维护 > 诊断中心”，选中“Ping”页签；在“目的主机的域名或 IP 地址”中输入“192.168.2.2”，单击“高级配置”，在“报文源地址”中输入“192.168.1.1”，单击“Ping”，结果显示应如下：

```
<USG-A>PING 192.168.2.2
56   data bytes, press CTRL_C to break
    Reply from 192.168.2.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 192.168.2.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 192.168.2.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 192.168.2.2: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 192.168.2.2: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 192.168.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/12/20 ms
```

从 USG-B 上使用源地址 192.168.2.2 Ping 192.168.1.1，结果应成功；

在 USG-B 上，选择“系统 > 维护 > 诊断中心”，选中“Ping”页签；在“目的主机的域名或 IP 地址”中输入“192.168.1.1”，单击“高级配置”，在“报文源地址”中输入“192.168.2.2”，单击“Ping”，结果显示应如下：

```
<USG-B>PING 192.168.1.1
56   data bytes, press CTRL_C to break
     Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=10 ms
     Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=20 ms
     Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=10 ms
     Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=10 ms
     Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=255 time=10 ms

   --- 192.168.1.1 ping statistics ---
     5 packet(s) transmitted
     5 packet(s) received
     0.00% packet loss
     round-trip min/avg/max = 10/12/20 ms
```

8.4 SA 实验

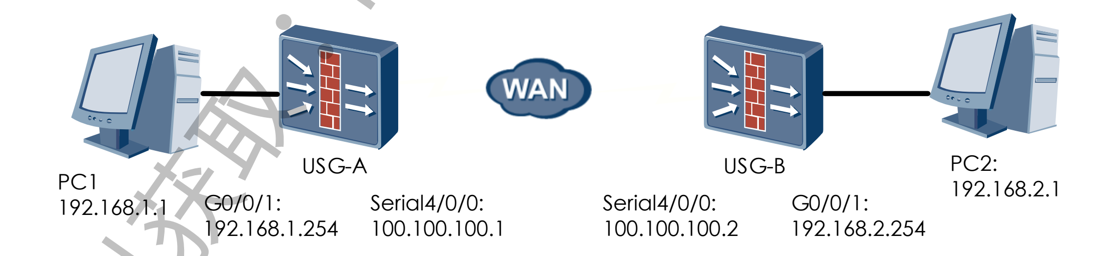
实验目的

为模拟广域网，在 USG 防火墙上安装 SA 接口卡，分别通过 WEB 和 CLI 这两种方式实现设备间互通；

组网设备

两台 USG2200，两台 PC，V35 线缆一根，网线两根。

实验拓扑图



实验步骤 – CLI

Step 1 分别配置防火墙 A 和防火墙 B Serial 4/0/0 接口的 IP 地址。

```
<USG-A->system-view
```

```
[USG-A]interface Serial 4/0/0
[USG-A-Serial4/0/0]ip address 100.100.100.1 255.255.255.0
<USG-B>system-view
[USG-B]interface Serial 4/0/0
[USG-B-Serial4/0/0]ip address 100.100.100.2 255.255.255.0
```

Step 2 重启接口，激活配置。

```
[USG-A-Serial4/0/0]shutdown
[USG-A-Serial4/0/0]undo shutdown

[USG-B-Serial4/0/0]shutdown
[USG-B-Serial4/0/0]undo shutdown
```

Step 3 将 Serial4/0/0 接口加入 Untrust 安全区域。

```
[USG-A]firewall zone untrust
[USG-A-zone-untrust]add interface Serial4/0/0
[USG-A-zone-untrust]quit

[USG-B]firewall zone untrust
[USG-B-zone-untrust]add interface Serial4/0/0
[USG-B-zone-untrust]quit
```

Step 4 接口 GigabitEthernet 0/0/1 加入 Trust 安全区域。

```
[USG-A]firewall zone trust
[USG-A-zone-trust]add interface GigabitEthernet 0/0/1
[USG-A-zone-trust]quit

[USG-B]firewall zone trust
[USG-B-zone-trust]add interface GigabitEthernet 0/0/1
[USG-B-zone-trust]quit
```

Step 5 配置域间缺省包过滤。

```
[USG-A]firewall packet-filter default permit all

[USG-B]firewall packet-filter default permit all
```

Step 6 配置缺省路由。

```
[USG-A]ip route-static 0.0.0.0 0.0.0.0 100.100.100.2

[USG-B]ip route-static 0.0.0.0 0.0.0.0 100.100.100.1
```

实验步骤 – WEB

Step 1 配置 USG-A 的接口 Serial 4/0/0。 选择“网络 > 接口 > 接口”。 在“接口列表”中单击 Serial 4/0/0 所在行的 ，依次输入或选择各项参数，具体参数配置如下：

网络 > 接口 > 接口

修改Serial

参数	值
接口名称	Serial4/0/0 *
别名	
VPN实例	public *
安全区域	untrust
链路层协议	◉ PPP ○ HDLC
类型	◉ 无 ○ 客户端 ○ 服务器
IP地址	100 . 100 . 100 . 1
子网掩码	255 . 255 . 255 . 0
NAT功能	☐ 启用
☐ 启用访问管理	☐ HTTP ☐ HTTPS ☐ Ping ☐ SSH ☐ SNMP ☐ Telnet

+ 高级

修改GigabitEthernet

参数	值
接口名称	GigabitEthernet0/0/1 *
别名	
VPN实例	public *
安全区域	trust
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	192 . 168 . 1 . 254 [IP地址详细配置]
子网掩码	255 . 255 . 255 . 0
默认网关	. . .
NAT功能	☐ 启用
☐ 启用访问管理	☐ HTTP ☐ HTTPS ☐ Ping ☐ SSH ☐ SNMP ☐ Telnet

Step 2 配置 USG-B（操作与 USG-A 相同，此处略。）

Step 3 USG-A 和 USG-B 上配置域间包过滤，以保证网络基本通信正常。 选择“防火墙 > 安全策略 > 转发策略”。 单击“untrust->trust”下的“默认”所在行的 。 选择“动作”为“permit”。 单击“应用”。

防火墙 > 安全策略 > 转发策略

新建转发策略

字段	值
源安全区域	untrust *
目的安全区域	trust *
源地址	请选择或输入IP地址 [多选]
目的地址	请选择或输入IP地址 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

单击“trust->untrust”下的“默认”所在行的 。选择“动作”为“permit”。

单击“应用”。

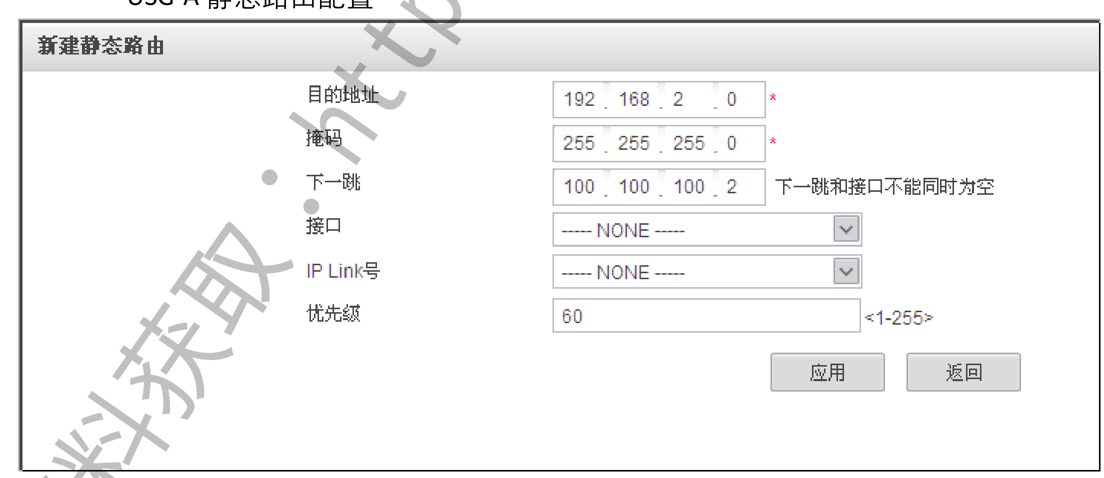
防火墙 > 安全策略 > 转发策略

新建转发策略

字段	值
源安全区域	trust *
目的安全区域	untrust *
源地址	请选择或输入IP地址 [多选]
目的地址	请选择或输入IP地址 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

Step 4 USG-A 和 USG-B 上路由配置，以保证网络基本通信正常。选择“路由 > 策略路由 > 策略路由”， 单击“新建”；依次选择或输入各项参数，单击“应用”。

USG-A 静态路由配置



USG-B 静态路由配置

路由 > 静态 > 静态路由

新建静态路由

目的地址	192 . 168 . 1 . 0	*
掩码	255 . 255 . 255 . 0	*
下一跳	100 . 100 . 100 . 1	下一跳和接口不能同时为空
接口	----- NONE -----	
IP Link号	----- NONE -----	
优先级	60	<1-255>

应用 返回

验证结果

从 USG-A 上使用源地址 192.168.1.1 Ping 192.168.2.2，结果应成功；

在 USG-A 上，选择“系统 > 维护 > 诊断中心”，选中“Ping”页签；在“目的主机的域名或 IP 地址”中输入“192.168.2.2”，单击“高级配置”，在“报文源地址”中输入“192.168.1.1”，单击“Ping”，结果显示应如下：

```
<USG-A>PING 192.168.2.2
56  data bytes, press CTRL_C to break
    Reply from 192.168.2.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 192.168.2.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 192.168.2.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 192.168.2.2: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 192.168.2.2: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 192.168.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/12/20 ms
```

从 USG-B 上使用源地址 192.168.2.2 Ping 192.168.1.1，结果应成功；

在 USG-B 上，选择“系统 > 维护 > 诊断中心”，选中“Ping”页签；在“目的主机的域名或 IP 地址”中输入“192.168.1.1”，单击“高级配置”，在“报文源地址”中输入“192.168.2.2”，单击“Ping”，结果显示应如下：

```
<USG-B>PING 192.168.1.1
56  data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=255 time=10 ms
```

```
--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/12/20 ms
```

8.5 3G 实验

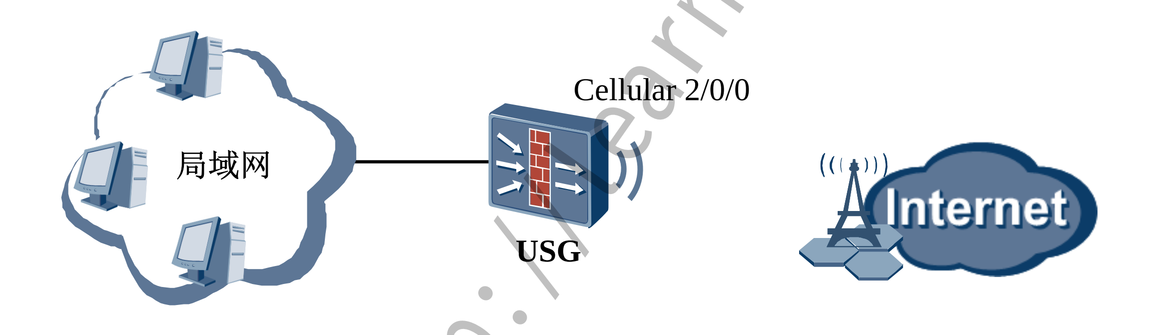
实验目的

在 USG 上安装了 3G 接口卡时，可以通过配置使内网用户通过 3G 方式连接到 Internet。

组网设备

USG2110-X 设备一台，USB 无线网卡一张，主机一台。

实验拓扑图



实验步骤

Step 1 配置接口基本参数。选择“网络 > 接口 > 接口”。 在“接口列表”中单击 GE0/0/1 所在行的 ，依次输入或选择各项参数，如图所示：

网络 > 接口 > 接口

修改GigabitEthernet

参数	值
接口名称	GigabitEthernet0/0/1 *
别名	
VPN实例	public *
安全区域	trust
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	10 . 1 . 1 . 1 （IP地址详细配置）
子网掩码	255 . 255 . 255 . 0
默认网关	. . .
NAT功能	☐ 启用
☐ 启用访问管理	☐ HTTP ☐ HTTPS ☐ Ping ☐ SSH ☐ SNMP ☐ Telnet

其他参数均为缺省值。单击“应用”。

Step 2 配置 3G 拨号。选择“无线&DSL > 3G > 3G 配置”。 在“基础配置”区域框中，配置参数如图所示。

参数	值
3G功能	☑ 启用
接入点名称	UNINET
用户名	user
密码	uesr
拨号串	*99# *
在线方式	○ 一直在线 ◉ 空闲自动断线（秒） 600 <1-65535>
安全区域	untrust *
NAT功能	☑ 启用

在“高级”区域框中，分别选择“自动获得 IP 地址”和“自动获得 DNS 地址”。单击“应用”。

Step 3 配置 DHCP，给内网 PC 分配 IP 地址。选择“网络 > DHCP 服务器 > 服务”。在“配置 DHCP 基本参数”中选择“启用”，单击“应用”，启用 DHCP 服务。

网络 > DHCP服务器 > 服务

配置DHCP基本参数

DHCP服务	☑ 启用	应用

在“DHCP 服务信息列表”中单击“新建”，依次输入或选择各项参数，具体参数如图所示：

参数	值
接口名称	GE0/0/1 *
服务类型	服务器
可分配IP地址范围	10.1.1.1 * - 10.1.1.254 *
子网掩码	255.255.255.0 *
默认网关	10.1.1.1 *
DNS服务	○ 利用系统的DNS设置 ● 指定
首选DNS服务器	. . .
备用DNS服务器	. . .

＋ 高级

应用 返回

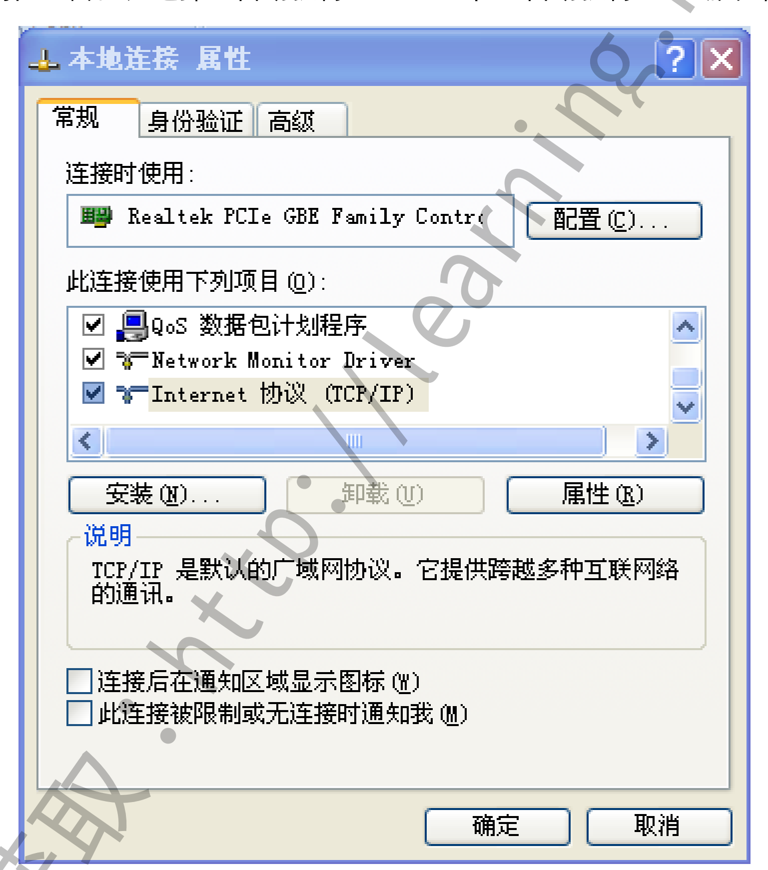
其他参数均为缺省值。单击“应用”。

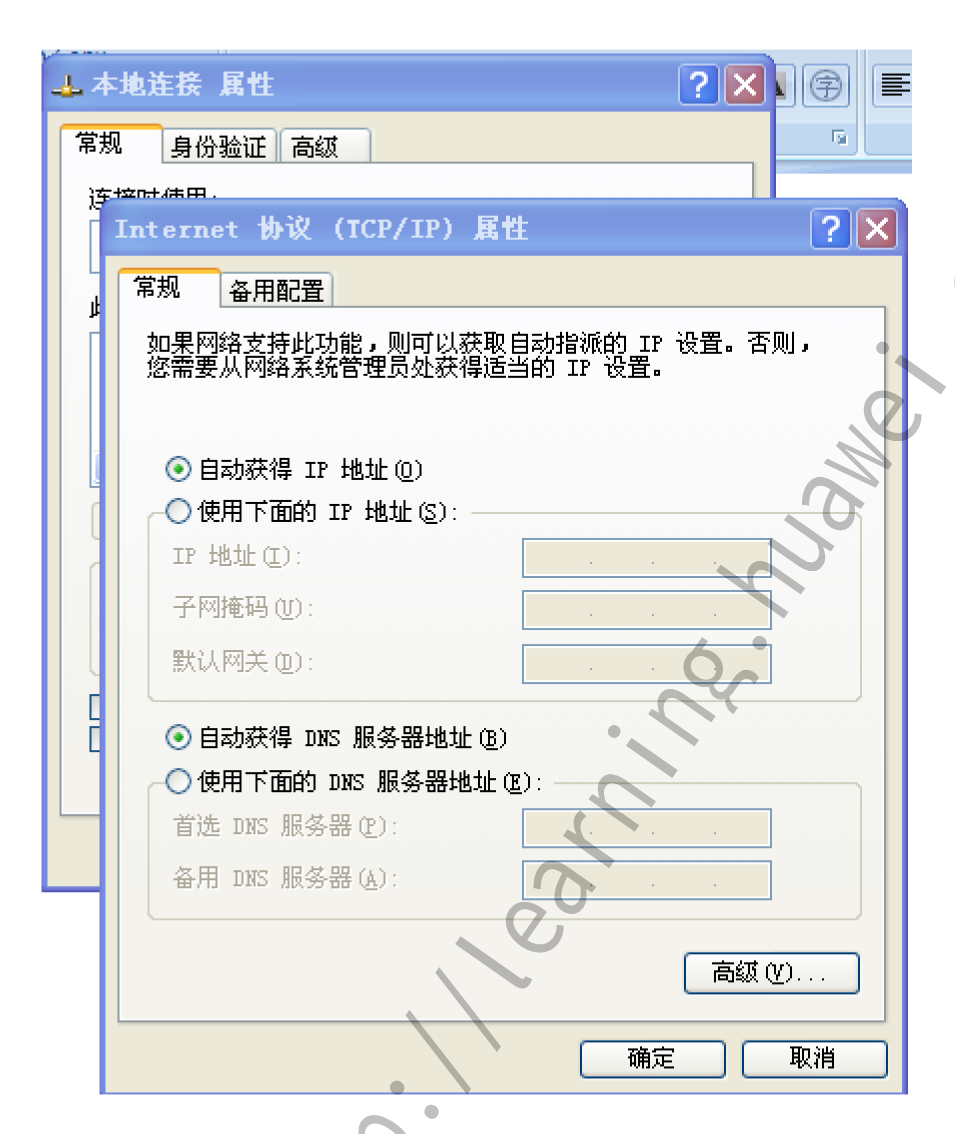
Step 4 配置域间包过滤，以保证网络基本通信正常。选择“防火墙 > 安全策略 > 转发策略”。在“转发策略列表”中查看 trust->untrust 默认规则的“动作”是否为 permit。如果不是，请单击 修改。

Step 5 配置 PC（PC 的操作系统以 Windows XP 为例）。右击桌面“网上邻居”，单击“属性”，进入“网络连接”窗口。选择连接时使用网卡对应的“本地连接”，右击“本地连接”，进入“本地连接属性”窗口。



选择“Internet 协议 (TCP/IP)”，点击“属性”，进入“Internet 协议 (TCP/IP) 属性”窗口，选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”。





验证结果

在 PC 上打开网页，检查是否可以正常上网。

选择“无线&DSL > 3G > 3G 配置”。查看“当前状态”和“信号强度”。如果显示“未连接”，表示 3G 拨号失败，请检查配置；如果“信号强度”弱，会影响连接速度，请调整天线或设备位置。

9 VPN 技术实验

9.1 L2TPVPN 实验（Client-Initialized VPN）

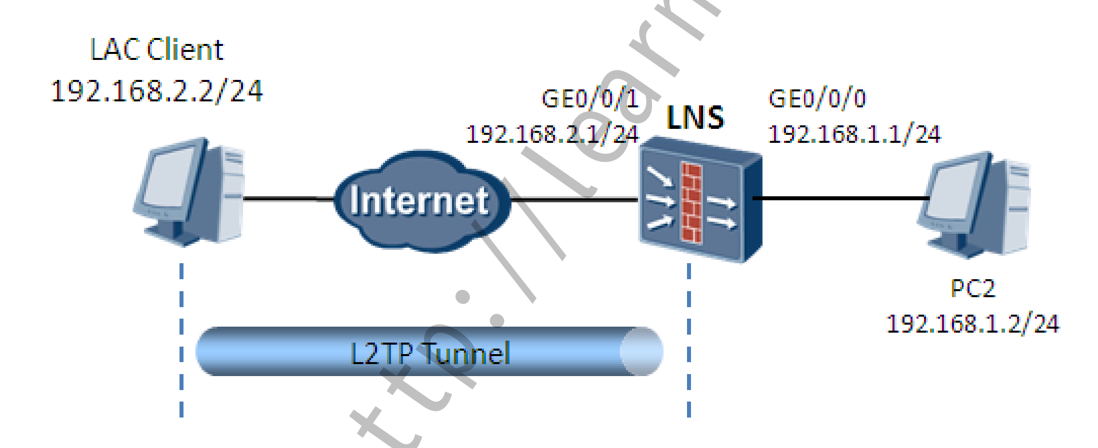
实验目的

通过该实验，你将能够掌握如何实现 Client-Initialized 方式建立本地认证的 L2TP 的配置。

组网设备

USG 防火墙一台，PC 机两台。

实验拓扑图



实验步骤-CLI

Step 1 配置 LNS 端，设置接口 IP 地址并配置域间包过滤策略。

```
<USG> system-view
[USG] sysname LNS
[LNS] interface GigabitEthernet 0/0/1
[LNS-GigabitEthernet0/0/1] ip address 192.168.2.1 255.255.255.0
[LNS-GigabitEthernet0/0/1] quit
[LNS] interface GigabitEthernet 0/0/0
[LNS-GigabitEthernet0/0/0] ip address 192.168.1.1 255.255.255.0
[LNS-GigabitEthernet0/0/0] quit
```

Step 2 创建虚拟模板 Virtual-Template 并配置相关信息。

```
[LNS] interface virtual-template 1
```

```
[LNS-Virtual-Template1] ip address 192.168.0.1 255.255.255.0
[LNS-Virtual-Template1] ppp authentication-mode chap
[LNS-Virtual-Template1] quit
```

Step 3 开启 L2TP。

```
[LNS] l2tp enable
```

Step 4 创建并配置 L2TP 组。

```
[LNS] l2tp-group 1
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1 remote client1
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password cipher Password123
```

Step 5 配置给用户分配的地址池。并设置用户名及口令（应与出差员工侧的设置一致）。

```
[LNS]aaa
[LNS-aaa] ip pool 1 192.168.0.2 192.168.0.100
[LNS-aaa] local-user vpdnuser password cipher Hello123
[LNS-aaa] quit
```

Step 6 配置为对端接口分配 IP 地址池中的地址。

```
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] remote address pool 1
[LNS-Virtual-Template1] quit
```

Step 7 将接口加入安全区域，并配置域间包过滤。

```
[LNC]firewall zone trust
[LNC-zone-trust]add interface GigabitEthernet 0/0/0
[LNC-zone-trust]add interface virtual-template 1
[LNC-zone-trust]quit
[LNC]firewall zone untrust
[LNC-zone-untrust]add interface GigabitEthernet 0/0/1
[LNC-zone-untrust]quit
[LNC]policy interzone untrust trust inbound
[LNC-policy-interzone-trust-untrust-inbound]policy 0
[LNC-policy-interzone-trust-untrust-inbound-0]action permit
```

Step 8 配置 LAC 客户端。在 LAC 主机上安装华为 secoway VPN Client。点击 新建 创建一个新的连接。选择通过参数创建连接，单击下一步：



Step 9 输入服务器地址，即 LNS 端地址，用户名和密码（vpdnuser/Hello123），完成后单击下一步。



Step 10 输入隧道名称（client1）和认证模式（CHAP）。勾选启用对到验证功能，并输入隧道验证密码（password123）。完成 L2tp 连接创建。

新建连接向导

第三步：请输入L2TP设置。

HUAWEI

隧道名称(M)： client1

认证模式(A)： CHAP

启用隧道验证功能(E)

隧道验证密码(T)： ***********

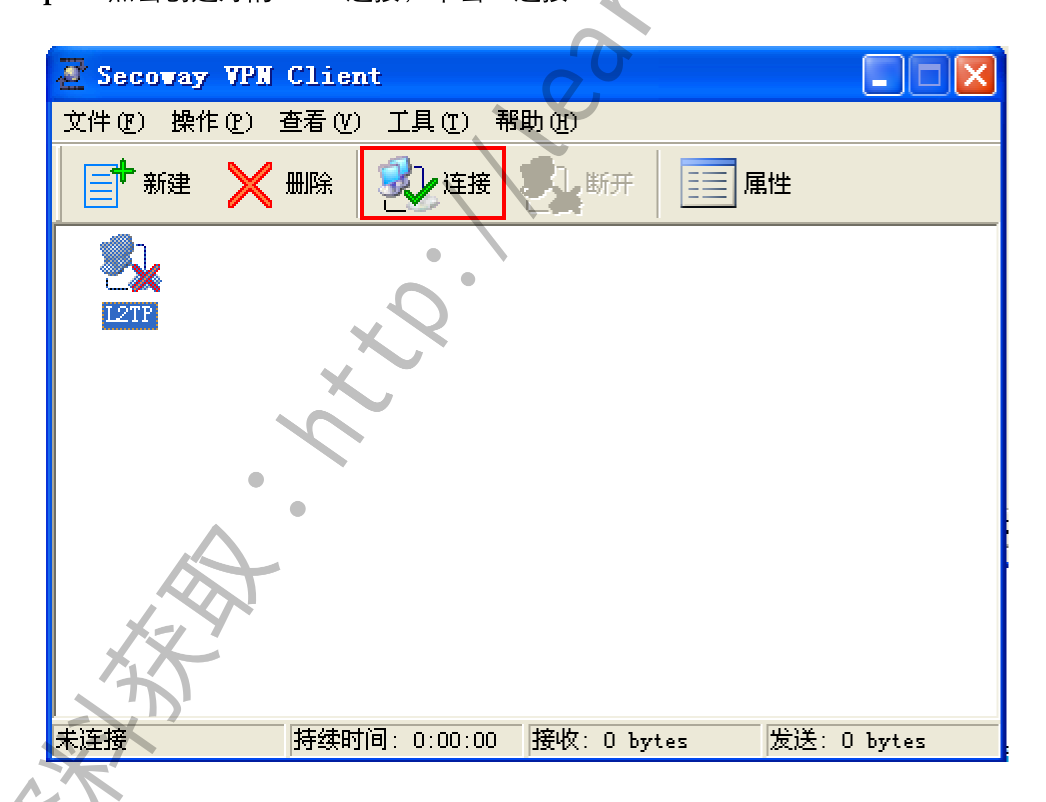
启用IPSEC安全协议(S)

预共享密钥(R)　数字签名(USBKey)

身份验证字：

<上一步(P)　下一步(N)>　完成(F)　取消(C)

Step 11 点击创建好的 L2TP 连接，单击“连接”。



实验步骤-Web

Step 1 配置 LNS 端，设置接口 IP 地址并配置域间包过滤策略。选择“网络 > 接口 > 接口”。在“接口列表”中，单击 GE0/0/1 对应的 。配置如图所示：

修改GigabitEthernet

接口名称	GigabitEthernet0/0/1 *
别名	
VPN实例	public *
安全区域	untrust
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	192 . 168 . 1 . 1 [IP地址详细配置]
子网掩码	255 . 255 . 255 . 0
默认网关	. . .

Step 2 选择“防火墙 > 安全策略 > 本地策略”。在“转发策略列表”中，单击“untrust->trust”下的“默认”所在行的 。在“修改转发策略”界面中，选择“动作”为“permit”。在“trust -> untrust”下也同样修改为“permit”。

源安全区域	untrust *
目的安全区域	trust *
源地址	any
目的地址	any
用户	any
服务	请选择服务
时间段	all
动作	permit *

[应用] [返回]

源安全区域	trust *
目的安全区域	untrust *
源地址	any
目的地址	any
用户	any
服务	请选择服务
时间段	all
动作	permit *

应用 返回

Step 3 配置 L2TP 参数。选择“VPN > L2TP > L2TP”。在“配置 L2TP”中，选中 L2TP 后的“启用”，单击“应用”。

配置L2TP

L2TP ☑启用 应用

Step 4 在“L2TP 组列表”中，单击“新建”。选择“组类型”为“LNS”。单击“新建”，新建用户 vpdnuser/Hello123。如图所示。

新建用户

用户名	vpdnuser *
密码	•••••••• *
	为提升密码安全性，建议密码至少包含以下字符中的3种：<A-Z>，<a-z>，<0-9>，特殊字符（例如!，$，#，%）；且密码不能与用户或者用户的倒序相同。
确认密码	•••••••• *
分配固定IP	. . .

确定 取消

Step 5 配置其余 L2TP 参数。“对端隧道名称”要和 LAC 端配置的“本端隧道名称”一致。对端隧道名称为 client1/Password123，如图所示。

组类型	○ LAC	◉ LNS
本端隧道名称		
对端隧道名称	client1	*
隧道密码认证	☑	
隧道密码	●●●●●●●●●●●●	*
确认隧道密码	●●●●●●●●●●●●	*
用户组	default	*

Step 6 设置服务器地址及地址池段。如图所示，最后“应用”保存配置。

用户地址分配设置

服务器地址	192 . 168 . 0 . 3	*
子网掩码	255 . 255 . 255 . 0	*
地址池起始IP	192 . 168 . 0 . 2	*
地址池结束IP	192 . 168 . 0 . 100	

高级

保活时间	60	<60-1000>秒
AVP隐藏功能	☐ 启用	
	☐ 强制LCP重协商	
	☑ 强制本端CHAP认证	

应用　返回

Step 7 配置 LAC 客户端。该步骤与 CLI 方式配置中 LAC 客户端配置一致，请参考 CLI 配置中 Step 8 – Step11。

验证结果

配置成功后，当有 VPN 用户上线时，分别在 LAC 和 LNS 上执行 display l2tp tunnel 命令可发现隧道建立成功。以 LNS 侧的显示为例：

```
[LNS] display l2tp tunnel
 Total tunnel = 1
 LocalTID RemoteTID RemoteAddress     Port   Sessions RemoteName
 1        1         192.168.2.2       1701   1        client1
```

LAC 执行 display l2tp session 命令可看到会话连接建立情况。以 LNS 侧的显示为例：

```
[LNS] display l2tp session
```

```
Total session = 1
LocalSID   RemoteSID   LocalTID
1          1           1
```

在使用 Web 界面进行配置时，选择 VPN > L2TP > 监控，查看建立起的 L2tp 会话信息。



单击会话数，可查看到会话的详细信息：



9.2 GRE VPN 实验

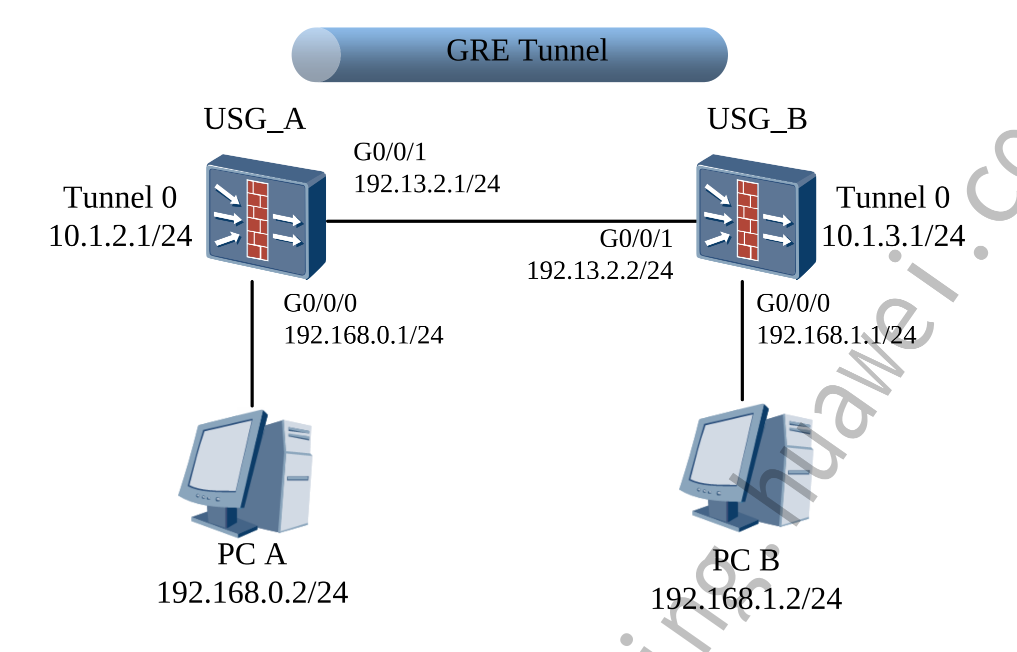
实验目的

通过本实验，你将学会如何配置 GRE VPN。

组网设备

USG 防火墙一台，PC 机两台。

实验拓扑图



实验步骤 - CLI

Step 1 配置主机 IP 地址，步骤省略。

Step 2 配置防火墙接口 IP 地址。

防火墙 A 配置

```
[USG_A]int GigabitEthernet 0/0/0
[USG_A-GigabitEthernet0/0/0]ip address 192.168.0.1 24
[USG_A-GigabitEthernet0/0/0]qu
[USG_A]int GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/1]ip add 192.13.2.1 30
```

防火墙 B 配置

```
[USG_B]int GigabitEthernet 0/0/0
[USG_B-GigabitEthernet0/0/0]ip address 192.168.1.1 24
[USG_B-GigabitEthernet0/0/0]qu
[USG_B]int GigabitEthernet 0/0/1
[USG_B-GigabitEthernet0/0/1]ip add 192.13.2.2 30
```

Step 3 配置接口安全区域并配置域间包过滤策略。

防火墙 A 配置

```
[USG_A]firewall zone trust
[USG_A-zone-trust]add interface GigabitEthernet 0/0/0
[USG_A-zone-trust]quit
[USG_A]firewall zone untrust
[USG_A-zone-untrust]add interface GigabitEthernet 0/0/1
```

```
[USG_A-zone-untrust]quit
[USG_A]firewall packet-filter default permit interzone trust untrust direction outbound
[USG_A]firewall packet-filter default permit interzone trust untrust direction inbound
```

防火墙 B 配置

```
[USG_B]firewall zone trust
[USG_B-zone-trust]add interface GigabitEthernet 0/0/0
[USG_B-zone-trust]quit
[USG_B]firewall zone untrust
[USG_B-zone-untrust]add interface GigabitEthernet 0/0/1
[USG_B-zone-untrust]quit
[USG_B]firewall packet-filter default permit interzone trust untrust direction outbound
[USG_B]firewall packet-filter default permit interzone trust untrust direction inbound
```

Step 4 配置 tunnel 接口。并将 tunnel 接口加入 untrust 区域。

防火墙 A 配置

```
[USG_A]interface Tunnel 0
[USG_A-Tunnel0]tunnel-protocol gre
[USG_A-Tunnel0]ip address 10.1.2.1 24
[USG_A-Tunnel0]source 192.13.2.1
[USG_A-Tunnel0]destination 192.13.2.2
[USG_A-Tunnel0]quit
[USG_A]firewall zone untrust
[USG_A-zone-untrust]add interface Tunnel 0
[USG_A-zone-untrust]quit
```

防火墙 B 配置

```
[USG_B]interface Tunnel 0
[USG_B-Tunnel0]tunnel-protocol gre
[USG_B-Tunnel0]ip address 10.1.3.1 24
[USG_B-Tunnel0]source 192.13.2.2
[USG_B-Tunnel0]destination 192.13.2.1
[USG_B-Tunnel0]quit
[USG_B]firewall zone untrust
[USG_B-zone-untrust]add interface Tunnel 0
[USG_B-zone-untrust]quit
```

Step 5 配置静态路由。

防火墙 A 配置

```
[USG_A]ip route-static 192.168.1.0 24 Tunnel 0
```

防火墙 B 配置

```
[USG_B]ip route-static 192.168.0.0 24 Tunnel 0
```

实验步骤 – Web

Step 1 配置主机 IP 地址，步骤省略。

Step 2 配置防火墙接口 IP 地址。选择“网络 > 接口 > 接口”。在“接口列表”中单击各接口对应的。配置如下图所示：配置完成后单击“应用”。

Step 3 防火墙 A 配置

接口名称	GigabitEthernet0/0/0 *	
别名		
VPN实例	public *	
安全区域	trust	
模式	● 路由 ○ 交换	
连接类型	● 静态IP ○ DHCP ○ PPPoE	
IP地址	192 . 168 . 0 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

接口名称	GigabitEthernet0/0/1 *	
别名		
VPN实例	public *	
安全区域	untrust	
模式	● 路由 ○ 交换	
连接类型	● 静态IP ○ DHCP ○ PPPoE	
IP地址	192 . 13 . 2 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

防火墙 B 配置

接口名称	GigabitEthernet0/0/0 *	
别名		
VPN实例	public *	
安全区域	trust	
模式	● 路由　○ 交换	
连接类型	● 静态IP　○ DHCP　○ PPPoE	
IP地址	192 . 168 . 1 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

接口名称	GigabitEthernet0/0/1 *	
别名		
VPN实例	public *	
安全区域	untrust	
模式	● 路由　○ 交换	
连接类型	● 静态IP　○ DHCP　○ PPPoE	
IP地址	192 . 13 . 2 . 2	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

Step 4 配置域间包过滤策略。选择“防火墙 > 安全策略 > 转发策略”。选择“转发策略”页签。在“转发策略列表”中单击 +。配置如下图所示：配置完成后单击“应用”。

防火墙 A 配置

源安全区域	trust *	
目的安全区域	untrust *	
源地址	请选择或输入IP地址	多选
目的地址	请选择或输入IP地址	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

防火墙 B 配置的配置与 A 相同。

Step 5 配置 tunnel 接口。并将 tunnel 接口加入 untrust 区域。选择 “VPN > GRE > GRE” 。在 “GRE 接口列表” 中，单击 “新建” 。配置 GRE 隧道接口参数，配置如下图所示：

防火墙 A 配置

接口名称	Tunnel 0 *	
安全区域	untrust *	
IP地址	10 . 1 . 2 . 1	
掩码	255 . 255 . 255 . 0	
隧道源IP配置方式	● IP地址	○ 接口
源IP地址	192 . 13 . 2 . 1	
隧道目的IP配置方式	● IP地址	○ 域名
目的IP地址	192 . 13 . 2 . 2	
隧道校验	☐ 启用	
隧道识别关键字		<0-4294967295>
	应用	返回

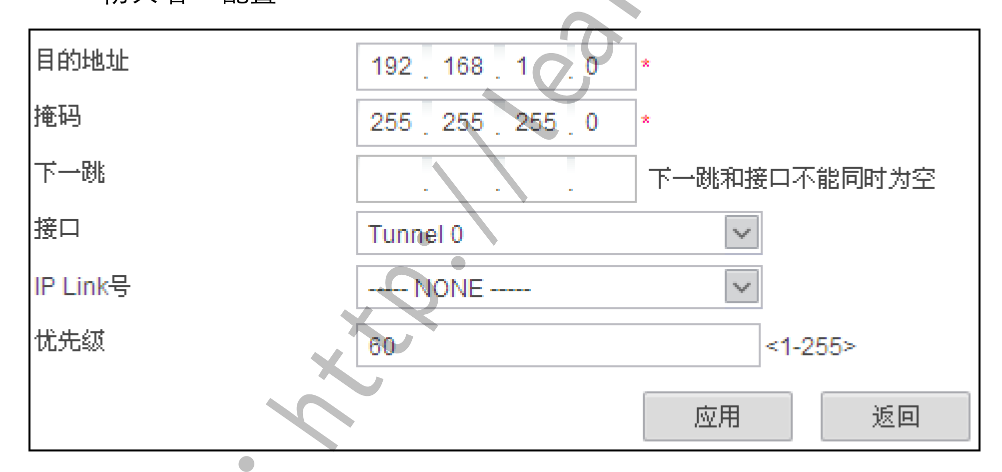
防火墙 B 配置

接口名称	Tunnel 0	*
安全区域	untrust	*
IP地址	10 . 1 . 3 . 1	
掩码	255 . 255 . 255 . 0	
隧道源IP配置方式	● IP地址	○ 接口
源IP地址	192 . 13 . 2 . 2	
隧道目的IP配置方式	● IP地址	○ 域名
目的IP地址	192 . 13 . 2 . 1	
隧道校验	☐ 启用	
隧道识别关键字		<0-4294967295>

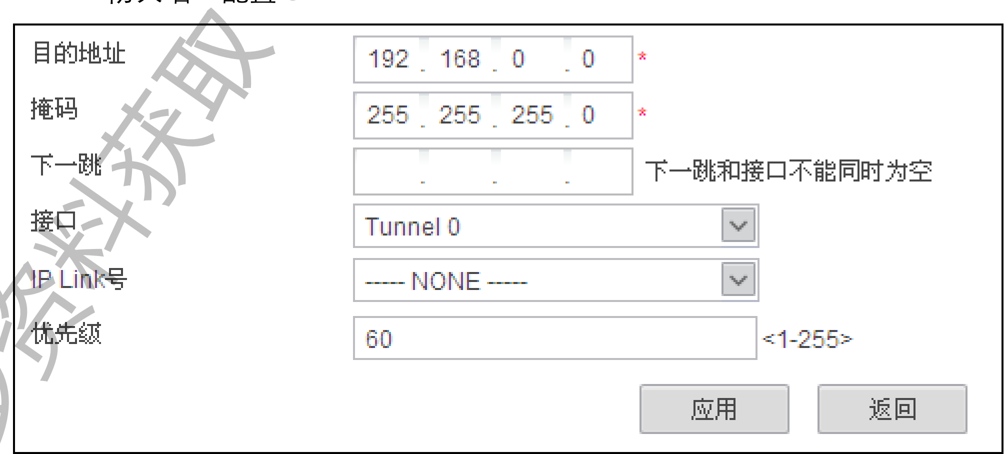
应用 返回

Step 6 配置静态路由。选择“路由 > 静态 > 静态路由”。在“静态路由列表”中，单击“新建”。在“新建静态路由”界面中，配置如下图所示：

防火墙 A 配置



防火墙 B 配置



验证结果

PCA 和 PCB 之间能够相互 ping 通。

10 IPSec VPN 实验

10.1 点到点的 IPSec 隧道实验

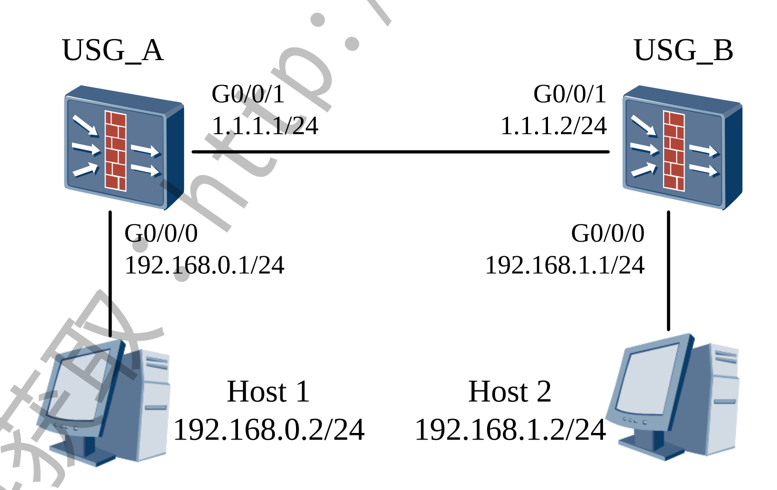
实验目的

掌握点对点方式，两端设备公网 IP 地址固定场景下 IPSec VPN 基本配置。

组网设备

USG2200/5000 防火墙 2 台，PC 机 2 台。

实验拓扑图



实验步骤 – CLI

配置 USG_A

Step 1 基础配置。（略）

Step 2 配置 Trust 域与 Untrust 域的域间缺省过滤规则。

```
[USG_A] firewall packet-filter default permit interzone trust untrust direction inbound
[USG_A] firewall packet-filter default permit interzone trust untrust direction outbound
```

Step 3 配置 USG_A 的 ACL，定义要保护的数据流。

```
[USG_A]acl 3000
[USG_A-acl-adv-3000]rule permit ip source 192.168.0.0 0.0.0.255 destination 1192.168.1.0 0.0.0.255
[USG_A-acl-adv-3000]quit
```

Step 4 配置到对端私网地址段的静态路由

```
[USG_A] ip route-static 192.168.1.0 255.255.255.0 1.1.1.2
```

Step 5 配置 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_A] ipsec proposal tran1
[USG_A-ipsec-proposal-tran1]encapsulation-mode tunnel
[USG_A-ipsec-proposal-tran1]transform esp
[USG_A-ipsec-proposal-tran1]esp authentication-algorithm md5
[USG_A-ipsec-proposal-tran1]esp encryption-algorithm des
[USG_A-ipsec-proposal-tran1]quit
```

Step 6 配置 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] authentication-method pre-share
[USG_A-ike-proposal-10] authentication-algorithm sha1
[USG_A-ike-proposal-10] integrity-algorithm hmac-sha1-96
[USG_A-ike-proposal-10] quit
```

Step 7 配置 IKE peer。

```
[USG_A]ike peer b
[USG_A-ike-peer-b]ike-proposal 10
[USG_A-ike-peer-b]remote-address 1.1.1.2
[USG_A-ike-peer-b]pre-shared-key abcde
[USG_A-ike-peer-b]quit
```

Step 8 配置安全策略。

```
[USG_A] ipsec policy map1 10 isakmp
[USG_A-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_A-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_A-ipsec-policy-isakmp-map1-10] ike-peer b
[USG_A-ipsec-policy-manual-map1-10] quit
```

Step 9 在接口上引用安全策略。

```
[USG_A] interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/1] ipsec policy map1
```

配置 USG_B

Step 10 基础配置。（略）

Step 11 配置 Trust 域与 Untrust 域的域间缺省过滤规则。

```
[USG_B] firewall packet-filter default permit interzone trust untrust direction inbound
[USG_B] firewall packet-filter default permit interzone trust untrust direction outbound
```

Step 12 配置 USG_B 的 ACL，定义要保护的数据流。

```
[USG_B]acl 3000
[USG_B-acl-adv-3000]rule permit ip source 192.168.1.0 0.0.0.255 destination 1192.168.0.0 0.0.00.255
[USG_B-acl-adv-3000]quit
```

Step 13 配置到对端私网网段的静态路由

```
[USG_B] ip route-static 192.168.0.0 255.255.255.0 1.1.1.1
```

Step 14 配置 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_B] ipsec proposal tran1
[USG_B-ipsec-proposal-tran1]encapsulation-mode tunnel
[USG_B-ipsec-proposal-tran1]transform esp
[USG_B-ipsec-proposal-tran1]esp authentication-algorithm md5
[USG_B-ipsec-proposal-tran1]esp encryption-algorithm des
[USG_B-ipsec-proposal-tran1]quit
```

Step 15 配置 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_B] ike proposal 10
[USG_B-ike-proposal-10] authentication-method pre-share
[USG_B-ike-proposal-10] authentication-algorithm sha1
[USG_B-ike-proposal-10] integrity-algorithm hmac-sha1-96
[USG_B-ike-proposal-10] quit
```

Step 16 配置 IKE peer。

```
[USG_B]ike peer a
[USG_B-ike-peer-b]ike-proposal 10
[USG_B-ike-peer-b]remote-address 1.1.1.1
[USG_B-ike-peer-b]pre-shared-key abcde
[USG_B-ike-peer-b]quit
```

Step 17 配置安全策略。

```
[USG_B] ipsec policy map1 10 isakmp
[USG_B-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_B-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_B-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_B-ipsec-policy-manual-map1-10] quit
```

Step 18 接口上引用安全策略。

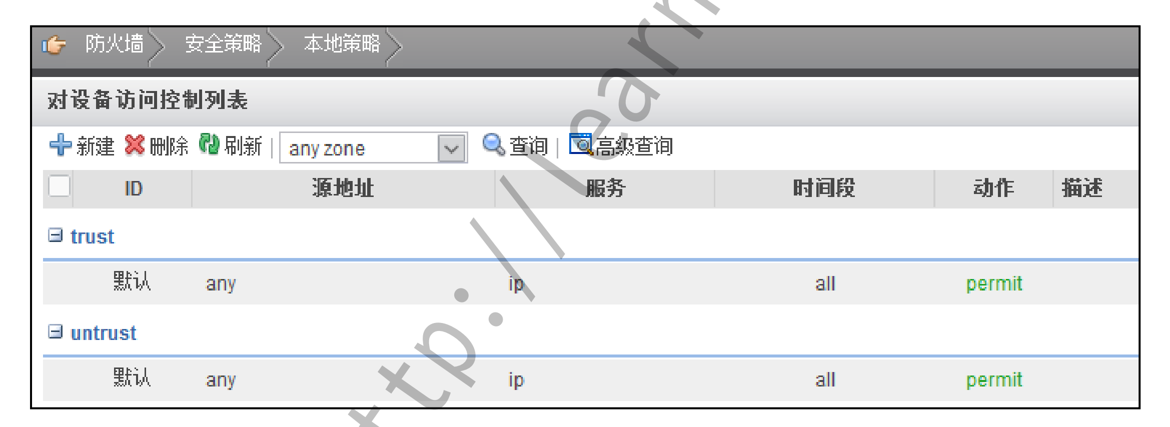
```
[USG_B] interface GigabitEthernet 0/0/1
[USG_B-GigabitEthernet0/0/1] ipsec policy map1
```

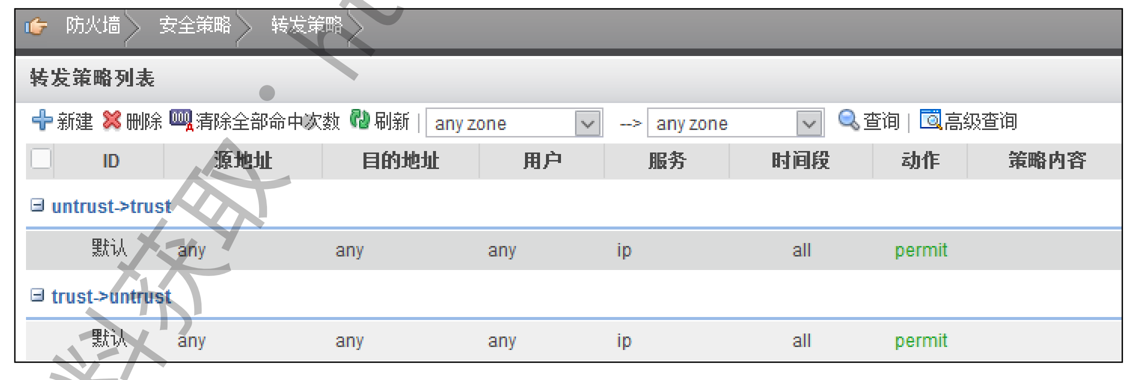
实验步骤 – Web

USG_A 配置

Step 1 基础配置。（略）

Step 2 配置 Trust 域与 Untrust 域的域间缺省过滤规则和 Local 安全区域和 Untrust 安全区域之间的安全策略。





Step 3 配置到对端私网网段的静态路由

路由 > 静态 > 静态路由

新建静态路由

目的地址	192 . 168 . 1 . 0 *
掩码	255 . 255 . 255 . 0 *
下一跳	1 . 1 . 1 . 2 下一跳和接口不能同时为空
接口	---- NONE ----
IP Link号	---- NONE ----
优先级	60 <1-255>

应用 返回

Step 4 配置 IKE 阶段 1 和阶段 2。选择 “VPN > IPSec > IKE 协商” 。 单击 “阶段 1” 。在“新建阶段 1”界面中，配置阶段 1 参数，其中“预共享密钥”设置为 abcde。单击 “应用” 。

VPN > IPSec > IKE协商

新建阶段1

阶段1	ike_a *
版本	V1 / V2 / ● V1 and V2
协商模式	● 主模式 / 野蛮模式
本地ID类型	IP
预共享密钥	●●●●● *
对端网关配置方式	指定对端网关
对端网关VPN实例	public
对端网关IP	1 . 1 . 1 . 2 * - . . .
对端地址池范围	. . . - . . .
VPN实例	public

+ 高级

应用 返回

Step 5 单击 “ike_a” 对应的+，创建 IKE 阶段 2。 在 “新建阶段 2” 界面中，配置阶段 2 参数单击 “应用” 。

VPN > IPSec > IKE协商

新建阶段2

阶段2	policy1 * - 1 *<1-10000>
阶段1	ike_a
备份阶段1	不指定备份阶段1
本端网关IP	. . .

+ 高级

应用 返回

Step 6 应用 IPSec 策略。选择 “VPN > IPSec > IPSec 策略” 。 单击 “新建” 。在“新建 IPSec 策略”界面中，配置需要 IPSec 隧道保护的数据流。单击“应用”。

VPN > IPSec > IPSec策略

新建IPSec策略

IPSec策略	policy1-1 *
数据流配置方式	◉ 指定数据流 ○ L2TP over IPSec
源地址	192.168.0.0/24
目的地址	192.168.1.0/24
服务	ip
动作	permit

应用 返回

Step 7 将IPSec策略与接口绑定，选择“VPN > IPSec > IPSec策略”。单击“policy1”后的 “应用接口 : - NONE - ” 。 在下拉列表中选择 GE0/0/1。 单击 “应用”。

VPN > IPSec > IPSec策略

IPSec策略列表

新建 删除 刷新 请输入IPSec策略名称 查询

源地址	目的地址	服务	动作
policy1 应用接口： - NONE - (1 Item)			
192.168.0.0\0.0.0.255	192.168.1.0\0.0.0.255	ip	permit

第 1 页共 1 页

配置应用的接口

配置接口 GE0/0/1

自动协商 启用

确定 取消

USG_B 配置与 USG_A 类似，仅需要修改静态路由、对端网关 IP 和需要 IPSec 隧道保护的数据流相应的 IP 地址即可，具体实验步骤略。

验证结果

配置成功后，从 PCA 可以 ping 通 PCB，分别在 USG_A 和 USG_B 上执行 **display ike sa**、**display ipsec sa** 会显示安全联盟的建立情况。以 USG_B 为例，出现以下显示信息说明 IKE 安全联盟、IPSec 安全联盟建立成功。

```
<USG_B> display ike sa
current ike sa number: 2
 ----------------------------------------------------------------------------------------------
     conn-id        peer                 flag          phase        vpn
 ----------------------------------------------------------------------------------------------
     101             1.1.1.1             RD            v2:2         public
     100             1.1.1.1             RD            v2:1         public

 flag meaning
 RD--READY       ST--STAYALIVE    RL--REPLACED          FD--FADING
 TO--TIMEOUT     TD--DELETING      NEG--NEGOTIATING    D--DPD
```

10.2 点到多点 IPSec 隧道实验

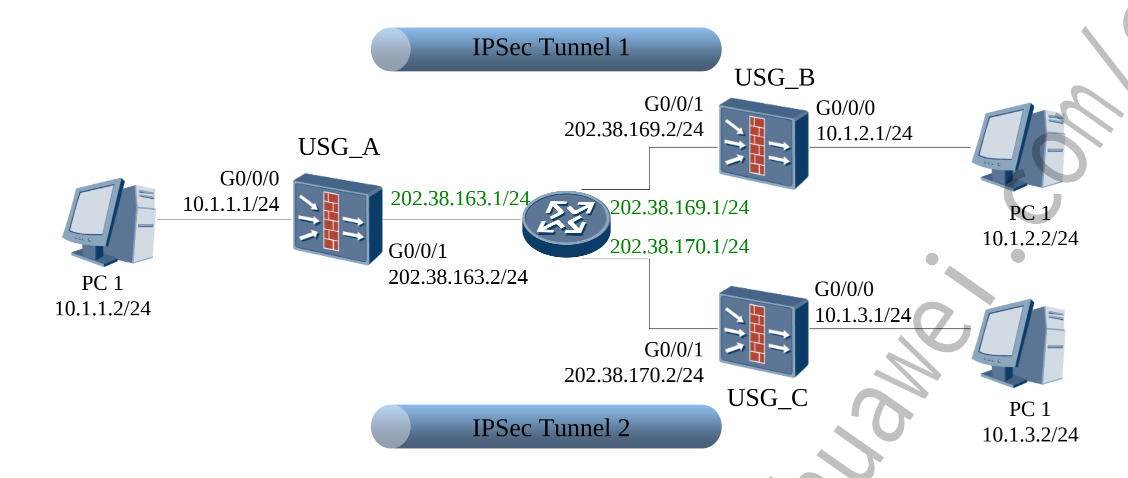
实验目的

掌握点到多点（总部到多个分支机构组网），分支机构 IP 地址不固定的场景下，总部通过 IKE 安全策略模板方式，分支机构通过 IKE 安全策略方式建立 IPSec 隧道的配置方法。

组网设备

USG2200/5000 防火墙 3 台，路由器或三层交换机 1 台，PC 机 3 台。

实验拓扑图



注：USG_B 和 USG_C 所在分支机构公网 IP 地址为动态获取，本实验中为方便组网配置固定 IP 地址。

实验步骤 - CLI

配置 USG_A

Step 1 基础配置。（略）

Step 2 配置到达分支机构的静态路由，此处假设下一跳地址为 202.38.163.1。

```
[USG_A] ip route-static 10.1.2.0 255.255.255.0 202.38.163.1
[USG_A] ip route-static 10.1.3.0 255.255.255.0 202.38.163.1
```

Step 3 定义被保护的数据流。

```
[USG_A] acl 3000
[USG_A-acl-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[USG_A-acl-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
[USG_A-acl-adv-3000] quit
```

Step 4 配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_A] ipsec proposal tran1
[USG_A-ipsec-proposal-tran1] encapsulation-mode tunnel
[USG_A-ipsec-proposal-tran1] transform esp
[USG_A-ipsec-proposal-tran1] esp authentication-algorithm md5
[USG_A-ipsec-proposal-tran1] esp encryption-algorithm des
[USG_A-ipsec-proposal-tran1] quit
```

Step 5 配置序号为 10 的 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] authentication-method pre-share
[USG_A-ike-proposal-10] authentication-algorithm sha1
[USG_A-ike-proposal-10] quit
```

Step 6 配置名称为 b 的 IKE Peer。

```
[USG_A] ike peer b
[USG_A-ike-peer-b] ike-proposal 10
[USG_A-ike-peer-b] pre-shared-key abcde
[USG_A-ike-peer-b] quit
```

Step 7 配置名称为 map_temp 序号为 1 的 IPSec 安全策略模板。

```
[USG_A] ipsec policy-template map_temp 1
[USG_A-ipsec-policy-templet-map_temp-1] security acl 3000
[USG_A-ipsec-policy-templet-map_temp-1] proposal tran1
[USG_A-ipsec-policy-templet-map_temp-1] ike-peer b
[USG_A-ipsec-policy-templet-map_temp-1] quit
```

Step 8 在 IPSec 安全策略 map1 中引用安全策略模板 map_temp。

```
[USG_A] ipsec policy map1 10 isakmp template map_temp
```

Step 9 在接口 GigabitEthernet 0/0/1 上应用安全策略 map1。

```
[USG_A] interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/2] ipsec policy map1
[USG_A-GigabitEthernet0/0/2] quit
```

配置 USG_B

Step 10 基础配置。（略）

Step 11 配置到达总部和其他私网的静态路由，下一跳地址为 202.38.169.1。

```
[USG_B] ip route-static 0.0.0.0 0.0.0.0 202.38.169.1
```

Step 12 定义被保护的数据流。

```
[USG_B] acl 3000
[USG_B-acl-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.255.255
[USG_B-acl-adv-3000] quit
```

Step 13 配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_B] ipsec proposal tran1
[USG_B-ipsec-proposal-tran1] encapsulation-mode tunnel
[USG_B-ipsec-proposal-tran1] transform esp
[USG_B-ipsec-proposal-tran1] esp authentication-algorithm md5
```

```
[USG_B-ipsec-proposal-tran1] esp encryption-algorithm des
[USG_B-ipsec-proposal-tran1] quit
```

Step 14 配置序号为 10 的 IKE 安全提议。(第 2 条命令开始为缺省配置可以不用配置)

```
[USG_B] ike proposal 10
[USG_B-ike-proposal-10] authentication-method pre-share
[USG_B-ike-proposal-10] authentication-algorithm md5
[USG_B-ike-proposal-10] quit
```

Step 15 配置 IKE Peer。

```
[USG_B] ike peer a
[USG_B-ike-peer-a] ike-proposal 10
[USG_B-ike-peer-a] remote-address 202.38.163.1
[USG_B-ike-peer-a] pre-shared-key abcde
[USG_B-ike-peer-a] quit
```

Step 16 配置名称为 map1 序号为 10 的 IPSec 安全策略。

```
[USG_B] ipsec policy map1 10 isakmp
[USG_B-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_B-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_B-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_B-ipsec-policy-isakmp-map1-10] quit
```

Step 17 在 GigabitEthernet 0/0/1 接口上应用安全策略 map1。

```
[USG_B] interface GigabitEthernet 0/0/1
[USG_B-GigabitEthernet0/0/2] ipsec policy map1
[USG_B-GigabitEthernet0/0/2] quit
```

配置 USG_C。

Step 18 基础配置。（略）

Step 19 配置到达总部和其他私网的静态路由，下一跳地址为 202.38.170.1。

```
[USG_C] ip route-static 0.0.0.0 0.0.0.0 202.38.170.1
```

Step 20 定义被保护的数据流。

```
[USG_C] acl 3000
[USG_C-acl-adv-3000] rule permit ip source 10.1.3.0 0.0.0.255 destination
10.1.1.0 0.0.255.255
[USG_C-acl-adv-3000] quit
```

Step 21 配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_C] ipsec proposal tran1
[USG_C-ipsec-proposal-tran1] encapsulation-mode tunnel
```

```
[USG_C-ipsec-proposal-tran1] transform esp
[USG_C-ipsec-proposal-tran1] esp authentication-algorithm md5
[USG_C-ipsec-proposal-tran1] esp encryption-algorithm des
[USG_C-ipsec-proposal-tran1] quit
```

Step 22 配置序号为 10 的 IKE 安全提议。(第 2 条命令开始为缺省配置可以不用配置)

```
[USG_C] ike proposal 10
[USG_C-ike-proposal-10] authentication-method pre-share
[USG_C-ike-proposal-10] authentication-algorithm md5
[USG_C-ike-proposal-10] quit
```

Step 23 配置 IKE Peer。

```
[USG_C] ike peer a
[USG_C-ike-peer-a] ike-proposal 10
[USG_C-ike-peer-a] remote-address 202.38.163.1
[USG_C-ike-peer-a] pre-shared-key abcde
[USG_C-ike-peer-a] quit
```

Step 24 配置名称为 map1 序号为 10 的 IPSec 安全策略。

```
[USG_C] ipsec policy map1 10 isakmp
[USG_C-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_C-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_C-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_C-ipsec-policy-isakmp-map1-10] quit
```

Step 25 在 GigabitEthernet 0/0/1 接口上应用安全策略 map1。

```
[USG_C] interface GigabitEthernet 0/0/1
[USG_C-GigabitEthernet0/0/2] ipsec policy map1
[USG_C-GigabitEthernet0/0/2] quit
```

实验步骤 - Web

USG_A 配置

Step 1 基础配置。（略）

Step 2 配置 Trust 域与 Untrust 域的域间缺省过滤规则和 Local 安全区域和 Untrust 安全区域之间的安全策略。


防火墙 > 安全策略 > 转发策略

转发策略列表

新建 删除 清除全部命中次数 刷新 | any zone --> any zone 查询 | 高级查询

ID	源地址	目的地址	用户	服务	时间段	动作	策略内容
untrust->trust							
默认	any	any	any	ip		all	permit
trust->untrust							
默认	any	any	any	ip		all	permit

防火墙 > 安全策略 > 本地策略

对设备访问控制列表

新建 删除 刷新 | any zone 查询 | 高级查询

ID	源地址	服务	时间段	动作	描述
trust					
默认	any	ip	all	permit	
untrust					
默认	any	ip	all	permit	

Step 3 配置到对端私网网段的静态路由（到两个分支机构）

路由 > 静态 > 静态路由

新建静态路由

目的地址	10 . 1 . 3 . 0 *
掩码	255 . 255 . 255 . 0 *
下一跳	202 . 38 . 163 . 1 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

路由 > 静态 > 静态路由

新建静态路由

目的地址	10 . 1 . 2 . 0 *
掩码	255 . 255 . 255 . 0 *
下一跳	202 . 38 . 163 . 1 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

Step 4 配置 IKE 阶段 1 和阶段 2。选择“VPN > IPSec > IKE 协商”。 单击“阶段 1”。在“新建阶段 1”界面中，配置阶段 1 参数，其中“预共享密钥”设置为 abcde 单击 “应用” 。

Step 5 单击 “ike_temp” 对应的+，创建 IKE 阶段 2。 在 “新建阶段 2” 界面中，配置阶段 2 参数，单击 “应用” 。

Step 6 应用 IPSec 策略。选择 “VPN > IPSec > IPSec 策略” 。 单击 “新建” 。在“新建 IPSec 策略”界面中，配置需要 IPSec 隧道保护的数据流，单击“应用”。

VPN > IPSec > IPSec策略

新建Rule

IPSec策略	map-1 *
数据流配置方式	● 指定数据流 ○ L2TP over IPSec
源地址	10.1.1.0/24
目的地址	10.1.2.0/24
服务	ip
动作	permit

应用 返回

Step 7 单击 “map-1” 后对应的 +，添加策略规则。单击 “应用”。配置完成后，同一条 IPSec 策略 map-1 中存在两条受保护数据流。

VPN > IPSec > IPSec策略

IPSec策略列表

新建 删除 刷新 | 请输入IPSec策略名称 查询

map 应用接口：- NONE - (2 Items)

源地址	目的地址	服务	动作	IPSec策略
10.1.1.0\0.0.0.255	10.1.2.0\0.0.0.255	ip	permit	map-1
10.1.1.0\0.0.0.255	10.1.3.0\0.0.0.255	ip	permit	map-1

第 1 页共 1 页

Step 8 将 IPSec 策略与接口绑定。选择“VPN > IPSec > IPSec 策略”。单击“map-1”后的 “应用接口：- NONE - ”。 在下拉列表中选择 GE0/0/1。 单击 “应用”。

配置应用的接口

配置接口	GE0/0/1
自动协商	☐ 启用

确定 取消

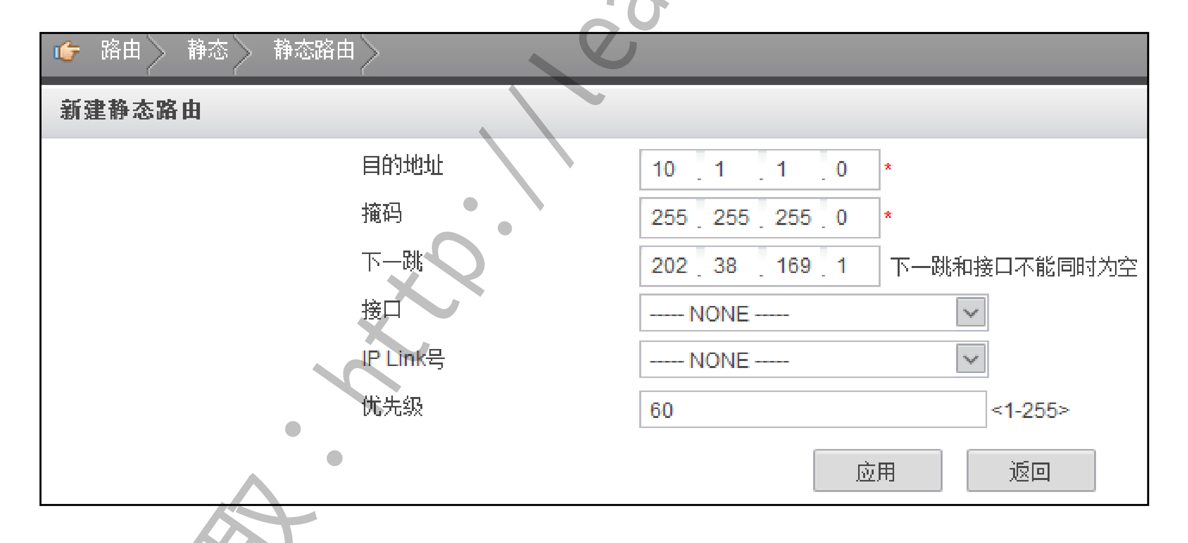
USG_B 配置

Step 9 基础配置。（略）

Step 10 配置 Trust 域与 Untrust 域的域间缺省过滤规则和 Local 安全区域和 Untrust 安全区域之间的安全策略。



Step 11 配置到对端私网网段的静态路由



Step 12 配置 IKE 阶段 1 和阶段 2。选择 “VPN > IPSec > IKE 协商” 。 单击 “阶段 1” 。在“新建阶段 1”界面中，配置阶段 1 参数，其中“预共享密钥”设置为 abcde。单击 “应用” 。

VPN > IPSec > IKE协商

修改阶段1

阶段1 ike_a *
版本 ○V1 ○V2 ●V1 and V2
协商模式 ●主模式 ○野蛮模式
本地ID类型 IP
预共享密钥 ••••• *
对端网关配置方式 固定地址
对端网关VPN实例 public
对端网关IP 202 . 38 . 163 . 2 *
对端地址池范围 . . . - . . .
VPN实例 public
+ 高级

应用 返回

Step 13 单击“ike_a”对应的+，创建 IKE 阶段 2。 在“新建阶段 2”界面中，配置阶段 2 参数。单击“应用”。

VPN > IPSec > IKE协商

新建阶段2

阶段2 map * - 1 *<1-10000>
阶段1 ike_a
备份阶段1 不指定备份阶段1
本端网关IP . . .
+ 高级

应用 返回

Step 14 应用 IPSec 策略。选择“VPN > IPSec > IPSec 策略”。 单击“新建”。在“新建 IPSec 策略”界面中，配置需要 IPSec 隧道保护的数据流。单击“应用”。

VPN > IPSec > IPSec策略

新建IPSec策略

IPSec策略	map-1 *
数据流配置方式	● 指定数据流 ○ L2TP over IPSec
源地址	10.1.2.0/24
目的地址	10.1.1.0/24
服务	ip
动作	permit

应用 返回

Step 15 将IPSec策略与接口绑定。选择"VPN > IPSec > IPSec策略"。单击"map-1"后的"应用接口：- NONE - "。 在下拉列表中选择 GE0/0/1。 单击"应用"。



USG_C 配置与 USG_B 类似，仅需要修改静态路由和需要 IPSec 隧道保护的数据流相应的 IP 地址即可，具体实验步骤略。

验证结果

在 PC2 和 PC3 上分别 ping PC1，都可以 ping 通。

分别在 USG_A、USG_B 和 USG_C 上执行 **display ike sa**、**display ipsec sa**，显示安全联盟的建立情况。

以 USG_B 为例，出现以下显示说明 IKE 安全联盟、IPSec 安全联盟建立成功。

```
<USG_B> display ike sa
current ike sa number: 2
  ---------------------------------------------------------------------------------
     conn-id      peer                 flag          phase      vpn
  ---------------------------------------------------------------------------------
     101          202.38.163.2         RD|ST         v2:2       public
     100          202.38.163.2         RD|ST         v2:1       public

  flag meaning
  RD--READY      ST--STAYALIVE   RL--REPLACED        FD--FADING
```

```
  TO--TIMEOUT   TD--DELETING    NEG--NEGOTIATING   D--DPD
<USG_B> display ipsec sa

  -----------------------------
  IPsec policy name: "map1"
  sequence number: 10
  mode: isakmp
  vpn: public
  -----------------------------
    connection id: 4
    rule number: 0
    encapsulation mode: tunnel
    tunnel local : 202.38.169.2      tunnel remote: 202.38.163.2
    flow          source: 10.1.2.0-10.1.2.255 0-65535 0
    flow destination: 10.1.1.0-10.1.1.255 0-65535 0

    [inbound ESP SAs]
      spi: 7519344 (0x72bc70)
      vpn: public          said: 8   cpuid: 0x0000
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887436044/3572
      max received sequence-number: 9
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 5365969 (0x51e0d1)
      vpn: public          said: 9   cpuid: 0x0000
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887435576/3572
      max sent sequence-number: 10
      udp encapsulation used for nat traversal: N
```

11 SSL VPN综合实验

11.1 Web代理/文件共享/端口转发/网络扩展

实验目的

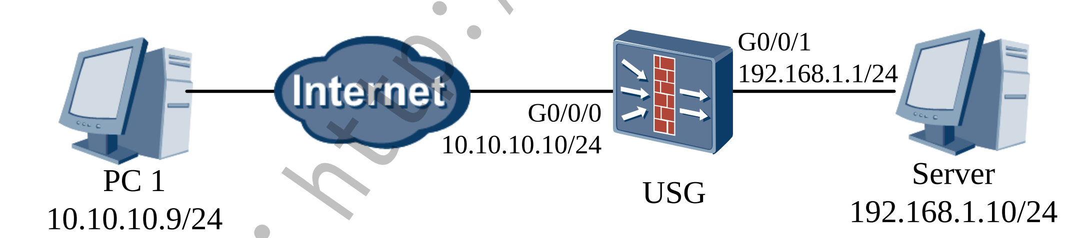
通过本次实验，你将能够学会配置以下功能：

- Web 代理
- 端口转发
- 文件共享
- 网络扩展

组网设备

PC 机两台，USG 防火墙一台。

实验拓扑图



实验步骤

Step 1 创建虚拟网关。

选择 VPN>SSL VPN>虚拟网关管理，点击 Add 新建一个虚拟网关，并取名为“Test”。

VPN > SSL VPN > 虚拟网关管理

虚拟网关名	Test *	字母、数字或下划线，1~15个字符
虚拟网关类型	独占	
IP地址	10 . 10 . 10 . 10 *	添加IP地址
虚拟网关域名		示例: www.company.com(独占型)，vt1.company.com(共享型)，www.company.com/aa(共享型)
HTTP重定向	启用HTTP重定向服务	
最大并发用户数		1~100，默认为系统限额（系统限额：100，当前剩余可用并发用户数：100）
最大用户数	1 *	1~1000，默认为1（系统限额：1000， 当前剩余可用用户数：1000）
最大资源数	1 *	1~1024，默认为1（系统限额：1024， 当前剩余可用资源数：1024）

应用 返回

Step 2 选择 VPN> SSL VPN>虚拟网关列表，选择刚刚创建的"Test"。

VPN > SSL VPN > 虚拟网关列表

虚拟网关列表

- 虚拟网关列表
  - test

虚拟网关详细信息

虚拟网关名	test
虚拟网关类型	独占型
IP地址	10 . 10 . 10 . 10
虚拟网关域名	
HTTP重定向	
最大并发用户数	
最大用户数	1
最大资源数	1
创建时间	2013/06/14 16:46:43

Step 3 创建用户账号。点击新建的虚拟网关"Test"前面的加号，展开列表，选择 **VPNDB 配置**， 点击 **新建** 新建一个测试用户 TestUser，密码为 password123。

VPN > SSL VPN > 虚拟网关列表

- 虚拟网关列表
  - test
    - 网络配置
    - SSL配置
    - 认证授权配置
    - 策略配置
    - VPNDB配置
    - 外部组配置

添加用户

用户名	TestUser
密码	●●●●●●●●●●●
确认密码	●●●●●●●●●●●
UID	
GID	
虚拟IP地址	. . .

Step 4 启用 Web 代理服务。点击新建的虚拟网关"Test"前面的加号，展开列表，选择 **Web 代理**，勾选"**启用**"并应用该设置。



在 **Web 代理资源管理**中，在 **web-link 资源**下，点击 新建 新建一个 Web 代理资源并将其应用。

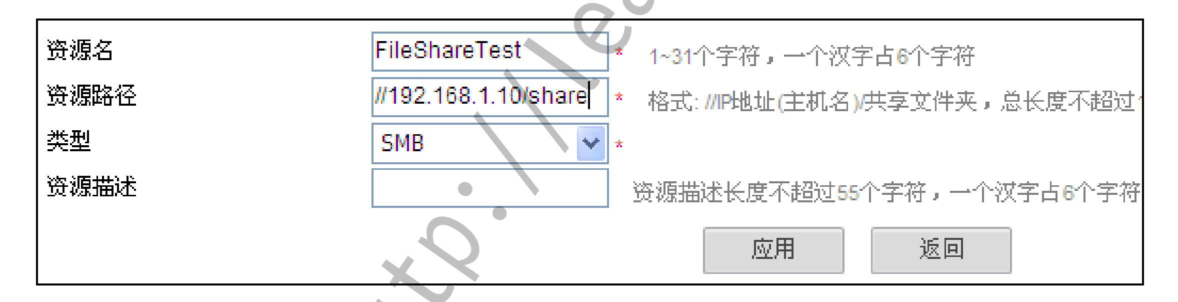


Step 5 启用文件共享服务。

点击新建的虚拟网关“Test”前面的加号，展开列表，选择**文件共享**。 勾选“启用”，并应用该设置。



在**文件共享资源管理**列表中，点击 **新建** 创建文件共享资源列表并应用。

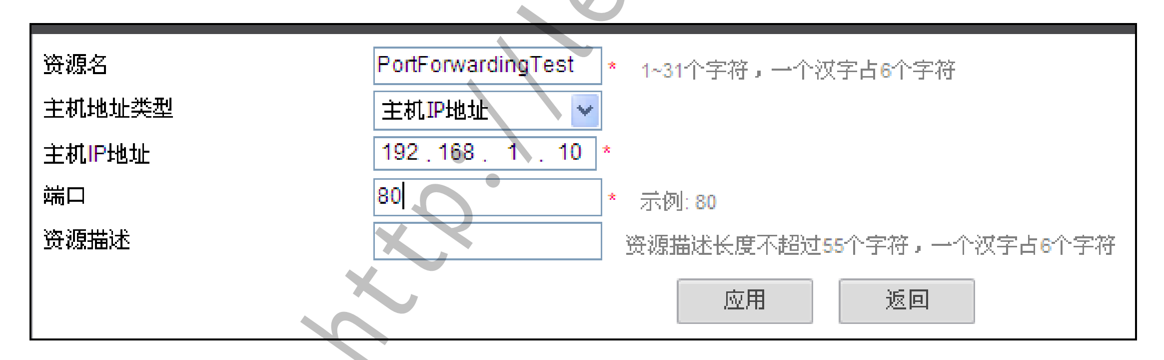


Step 6 启用端口转发服务。

点击新建的虚拟网关“Test”前面的加号，展开列表，选择**端口转发**。启用端口转发服务并应用。



在**端口转发资源管理**中，点击 新建 添加新的端口转发资源并应用设置。



Step 7 启用网络扩展服务。

点击新建的虚拟网关“Test”前面的加号，展开列表，选择**网络扩展**。勾选“启用”。



在客户端 IP 分配方式中使用 IP 地址池方式。设置好起始地址和结束地址。(192.168.1.20/24 – 192.168.1.30/24)



选择分离模式作为客户端路由模式，其余的配置为默认配置。最后应用设置并保存所有配置。



实验结果

在浏览器中输入 https://10.10.10.10 进入 SVN SSL VPN 界面，使用创建的测试账号进行登录。

Huawei Symantec

welcome

用户名: TestUser

密 码: ●●●●●●●●●●●●

选择语言 中 文

登 录

下载并安装证书可以为您消除安全警告提示框，并有助于加快您的访问速度。如何安装证书？ 点此下载证书
如果您使用的是USB Key证书认证，请先插入USB Key再访问本页面或插入USB Key后刷新本页面。

登录成功后，你将会看到之前所配置的 Web 代理、文件共享、端口转发和网络扩展服务。

Huawei Symantec 主页 帮助 注销

当前用户：TestUser 登录时间：2013-06-14 17:10:55 Web链接地址 浏 览

welcome

Web代理

Test Web Server

文件共享

fileShareTest

端口转发

启 动

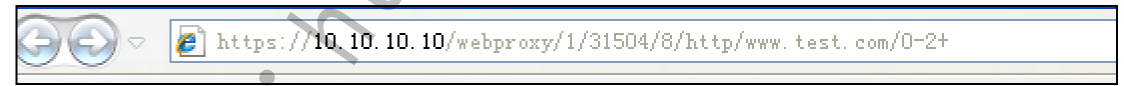
点击按钮启动业务后可以访问以下资源。

网络扩展

启 动

点击按钮启动业务后可以访问内网资源。

点击 Test Web Server，另外一个窗口将会弹出，而该测试服务器的地址会被添加上 SVN 设备的地址。



点击文件共享资源，登录文件共享服务器获取文件资源。

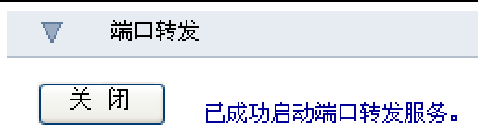
文件共享登录

用户名:

密码:

确 定

在端口转发服务下，点击"Start" 启用端口转发服务，尝试用 telent 的方式登录测试服务器。验证端口转发结果。



在网络扩展服务下启动网络扩展服务。



启动过后，检查本机 IP 地址，你将会发现 SVN 从 IP 地址池中分配了一个 IP 地址。



12 UTM 实验

12.1 UTM 病毒库、IPS 签名库升级

实验目的

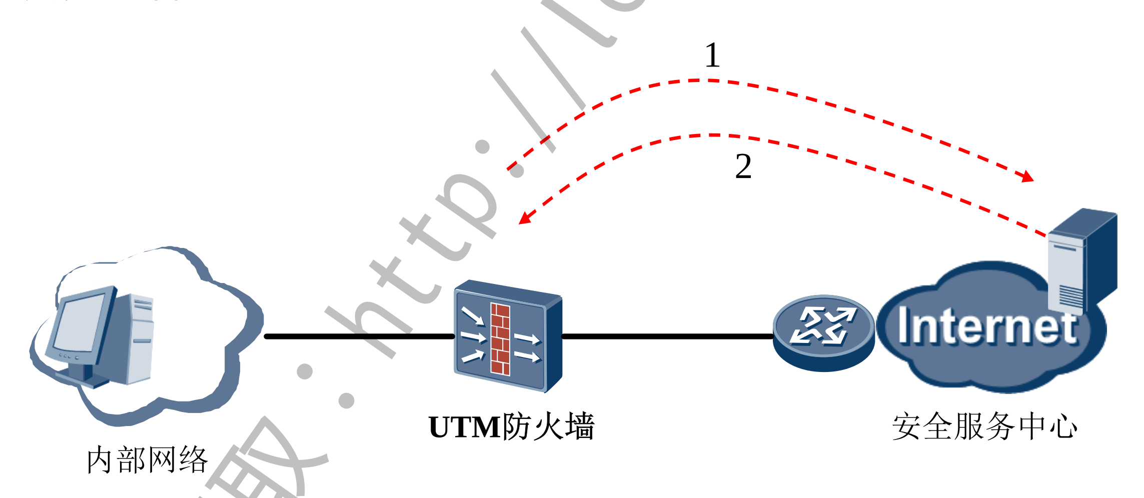
熟练掌握通过（CLI）或（WEB）在 USG 上配置 IPS 签名库和 AV 病毒库定时在线升级功能：

1. 通过安全服务中心定时在线升级 USG 上的 AV 病毒库、IPS 签名库；
2. 配置 IPS 的定时在线升级功能开启，升级时间为每天 02：00；
3. 配置 AV 的定时在线升级功能开启，升级时间为每天 01：00。

组网设备

1. USG2000/5000 防火墙一台（V3R1 版本），PC 一台
2. 要求防火墙能够连接互联网

实验拓扑图



项目	设备	数据
(1)	USG（待升级签名库和病毒库设备）	接口号：GigabitEthernet 0/0/0 IP 地址：192.168.17.3/24 安全区域：Trust
(2	USG（待升级签名库和病毒库设备）	下一跳 IP 地址：192.168.17.254 防火墙能够连接互联网

实验步骤 - CLI

Step 1 防火墙基础配置

在防火墙上配置 IP 地址，并将接口加入安全区域；配置缺省路由。配置略。
在防火墙上配置策略允许与安全服务中心的通信。配置略

Step 2 配置运行模式为 UTM 模式

```
<USG> system-view
[USG] runmode utm
```

注意：切换运行模式需要重启设备后才生效。请根据系统提示操作，推荐选择保存配置后重启。

Step 3 配置通过安全服务中心升级。

配置安全服务中心的域名。

```
[USG] security server domain sec.huawei.com
```

启用 DNS 服务器的域名解析功能。

```
[USG] dns resolve
```

配置 DNS 服务器的 IP 地址

```
[USG] dns server 61.139.2.69
```

Step 4 配置 USG 定时在线升级。

启用定时在线升级。

```
[USG] update schedule ips enable
[USG] uupdate schedule av enable
```

配置 IPS 和 AV 的每天定时在线升级的时间

```
[USG] update schedule ips daily 02：00
[USG] update schedule AV daily 01：00
```

安装新下载的签名库版本

```
[USG] update apply ips
```

实验步骤 – Web

Step 1 开启 UTM 功能。进入 web 管理界面—>UTM->基本配置->基本配置。在启用前边打上‘’，并点击“应用”



Step 2 配置安全服务中心。选择“系统 > 维护 > 升级中心”。不选中“内网升级”对应的“开启”。在“安全服务中心域名”中，输入需配置的安全服务中心的域名 sec.huawei.com。

系统 > 维护 > 升级中心

升级中心

内网升级 开启

安全服务中心域名 sec.huawei.com *

激活码 输入激活码 导入激活码文件

gPatj+lodZE3LT7FPXxZOsotwJKfr
VlSVo8vfQ2I8DVdzL0HFxwaAgaJ
E9tV7r5mPr/d6dol9Ub+hronznw/h
59+vQpOoM9UMpW2VT1Hx1kTE
XMYIAjgsQ6NtZK8uHsDx2iwDTjZ

激活

Step 3 添加 DNS 服务器。选择“网络 > DNS > DNS”。在“服务器列表”的文本框中输入 DNS 服务器的 IP 地址。单击“添加”。

网络 > DNS > DNS

服务器列表

删除 刷新 61 . 139 . 2 . 69 添加

IP	获取方式
61.139.2.69	STATIC

Step 4 配置 USG 定时在线升级。选择“系统 > 维护 > 升级中心”。选择“反病毒”或“入侵防御”。在定时在线升级前 ☑，输入每日升级时间，点击“应用”。

在线升级

☑ 定时在线升级 手动在线升级

每日 02 : 00 *

每周

在线升级

☑ 定时在线升级 手动在线升级

每日 01 : 00 *

每周

实验结果

实验结果：(CLI 方式)

1)，执行命令 display update configuration，查看内网升级的相关信息。

```
<USG2200>display update configuration
11:04:44  2013/06/09
```

```
==============Update configuration information==============
  Internal update mode            : Disable
  Internal update server          : -
  Internal update port            : -
  IPS                 :
    Application confirmation   : Disable
    Schedule update                 : Enable
    Schedule update frequency : Daily
    Schedule update time          : 02:00
  AV                   :
    Schedule update                 : Enable
    Schedule update frequency : Daily
    Schedule update time          : 01:00
==============================================================
```

2），执行命令 **display ips version 和 display av version**，可查看升级后的签名库或病毒库的版本。如果升级后的版本符合要求，表明升级成功。

```
<USG2200> display ips version
11:05:57   2013/06/09
==================Update information list===================
  Current version :
    Version number                  : 20130606.011
    Engine version                  : 4.5.6.37
    Engine size                     : 5757574 bytes
    Signature database version      : 20130606.011
    Signature database size         : 696352 bytes
    Update time                     : 09:00:32 2013/06/09
    Issue time of the update file : 07:44:08 2013/06/06

  Backup version :
    Version number                  : 20130522.011
    Engine version                  : 4.5.6.37
    Engine size                     : 5757574 bytes
    Signature database version      : 20130522.011
    Signature database size         : 695019 bytes
    Update time                     : 17:01:57 2013/06/08
    Issue time of the update file : 04:49:34 2013/05/22

  Factory default version :
    Version number                  : 0.000
    Engine version                  : 0.0.0.0
    Engine size                     : 0 bytes
```

```
      Signature database version       : 0.000
      Signature database size          : 0 bytes
      Update time                      : 00:00:00 0000/00/00
      Issue time of the update file : 00:00:00 0000/00/00
==============================================================

<USG2200>display av version
11:06:56  2013/06/09
==================Update information list====================
   Current version :
      Version number                   : 20130608.009
      Engine version                   : 1.1.1.4
      Engine size                      : 4106904 bytes
      Signature database version       : 20130608.009
      Signature database size          : 111325927 bytes
      Update time                      : 08:48:44 2013/06/09
      Issue time of the update file : 16:29:53 2013/06/08

   Backup version :
      Version number                   : 20130527.004
      Engine version                   : 1.1.1.4
      Engine size                      : 4106904 bytes
      Signature database version       : 20130527.004
      Signature database size          : 111538965 bytes
      Update time                      : 17:45:41 2013/06/08
      Issue time of the update file : 09:57:49 2013/05/27

   Factory default version :
      Version number                   : 0.000
      Engine version                   : 0.0.0.0
      Engine size                      : 0 bytes
      Signature database version       : 0.000
      Signature database size          : 0 bytes
      Update time                      : 00:00:00 0000/00/00
      Issue time of the update file : 00:00:00 0000/00/00
==============================================================
```

实验结果：(WEB 方式)

查看反病毒版本信息



查看入侵防御版本信息

反病毒

版本号：	20130608.009
引擎版本：	1.1.1.4
引擎大小：	4106904 bytes
签名库版本：	20130608.009
签名库大小：	111325927 bytes
升级时间：	08:48:44 2013/06/09
升级文件发布时间：	16:29:53 2013/06/08
版本回退	出厂版本

12.2 UTM 入侵防御实验

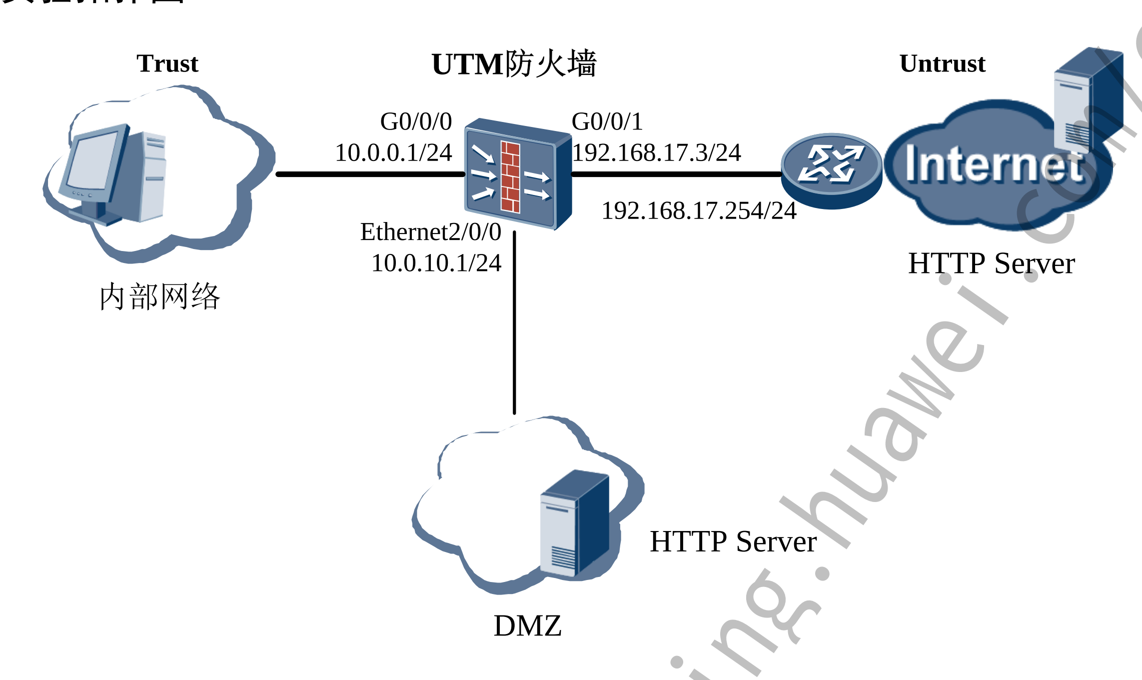
实验目的

使用（CLI）或（WEB）在 USG 上配置 IPS 功能，保护企业内部网络的 PC 和 HTTP 服务器避免受到来自 Internet 的攻击。

组网设备

1. USG2000/5000 防火墙一台（V3R1 版本），PC 一台
2. 要求防火墙能够访问互联网

实验拓扑图



实验步骤 - CLI

Step 1 配置运行模式为 UTM 模式。

```
<USG> system-view
[USG] runmode utm
```

注意：切换运行模式需要重启设备后才生效。请根据系统提示操作，推荐选择保存配置后重启。

Step 2 配置 USG 的基本配置（略）。

需要注意，为使防火墙能够接入互联网，需要配置缺省路由，下一跳地址为 Internet 上与 USG 直接相连的路由器接口的 IP 地址。

```
[USG] ip route-static 0.0.0.0 0 192.168.17.254
```

Step 3 启用 IPS 功能，并配置 IPS 的工作模式为 protective 使阻断响应生效。

```
[USG] ips enable
[USG] ips mode protective
```

配置 IPS 策略保护内部网络的 HTTP 服务器。

a. 创建 IPS 策略。创建 IPS 策略 protecthttp。

```
[USG] ips policy protecthttp
```

b. 在 IPS 策略中创建预定义签名的签名集，并配置签名集的启用状态和响应方式。

创建签名集 abc。

```
[USG-ips-policy-protecthttp] signature-set abc
```

配置将方向为 to-server 的签名加入签名集中。

```
[USG-ips-policy-protecthttp-signset-abc] direction enable
```

```
[USG-ips-policy-protecthttp-signset-abc] direction to-server
```

配置将严重性大于等于于 critical 的签名加入签名集中。

```
[USG-ips-policy-protecthttp-signset-abc] severity enable
[USG-ips-policy-protecthttp-signset-abc] severity above critical
```

配置将协议为 HTTP 的签名加入签名集中。

```
[USG-ips-policy-protecthttp-signset-abc] protocol enable
[USG-ips-policy-protecthttp-signset-abc] protocol http
```

启用签名集，并配置响应方式为 block。

```
[USG-ips-policy-protecthttp-signset-abc] signature-set enable
[USG-ips-policy-protecthttp-signset-abc] signature-set action block
[USG-ips-policy-protecthttp-signset-abc] return
```

Step 4 配置 IPS 策略保护内部网络 PC。创建 IPS 策略 protectpc，在 IPS 策略中引入 default 策略模板。

```
<USG> system-view
[USG] ips policy protectpc copy-from template default
[USG-ips-policy-protectpc] quit
```

Step 5 应用 IPS 策略。

把 IPS 策略 protecthttp 应用在 DMZ 和 Untrust 域间的 Inbound 方向。

```
[USG] policy interzone dmz untrust inbound
[USG-policy-interzone-dmz-untrust-inbound] policy 0
[USG-policy-interzone-dmz-untrust-inbound-0] policy service service-set http
[USG-policy-interzone-dmz-untrust-inbound-0] policy destination 10.0.10.0
0.0.0.255
[USG-policy-interzone-dmz-untrust-inbound-0] action permit
[USG-policy-interzone-dmz-untrust-inbound-0] policy ips protecthttp
[USG-policy-interzone-dmz-untrust-inbound-0] return
```

把 IPS 策略 protectpc 应用在 Trust 和 Untrust 域间的 Outbound 方向。

```
<USG> system-view
[USG] policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound] policy 1
[USG-policy-interzone-trust-untrust-outbound-1] policy service service-set http
[USG-policy-interzone-trust-untrust-outbound-1] policy source 10.0.0.0 0.0.0.255
[USG-policy-interzone-trust-untrust-outbound-1] action permit
[USG-policy-interzone-trust-untrust-outbound-1] policy ips protectpc
```

实验步骤 - Web

Step 1 完成防火墙基础配置（略）

Step 2 配置运行模式为 UTM 模式。选择“UTM > 基本配置 > 基本配置”。 选中“启动”。 单击“应用”。 选择“保存配置并重启”或“直接重启”，单击“确定”。

推荐选择“保存配置并重启”，先保存配置再重启设备，否则设备重启后，未保存的配置信息将丢失。



Step 3 配置静态路由，下一跳为 Internet 上与 USG 直接连接的路由器接口 IP 地址。选择“路由 > 静态 >静态路由”。 选择“新建”。 输入下一跳地址。单击“应用”。

路由 > 静态 > 静态路由

新建静态路由

目的地址 0 . 0 . 0 . 0

掩码 0 . 0 . 0 . 0

下一跳 192 . 168 . 17 . 254 下一跳和接口不能同时为空

接口 ----- NONE -----

IP Link号 ----- NONE -----

优先级 60 <1-255>

应用 返回

Step 4 开启 IPS 功能，并配置 IPS 模式。选择“UTM > 入侵防御 > 策略”。 在“配置全局参数”区域框中，配置参数如下：

1. 入侵防御功能开关：启用
2. 工作模式：防护模式
3. 特权策略：NONE
4. 单击“应用”。



Step 5 配置 IPS 策略保护内网网络的 HTTP 服务器

创建 IPS 策略 protecthttp。 选择“UTM > 入侵防御 > 策略”。单击“新建”，指定策略的名称为 protecthttp。单击“应用”。

UTM > 入侵防御 > 策略

IPS策略　策略模板

新建入侵防御策略

名称　protecthttp *

描述　IPS policy

同步策略/策略模板　-- 无 --

配置完成后请务必点击**应用**。

应用　返回

在策略中创建签名集，并配置签名集的启用状态和响应方式。在“签名集列表”区域中单击“新建”。在“新建签名集”中配置参数。单击“应用”。



应用 IPS 策略。选择“防火墙 > 安全策略 > 转发策略”。在“转发策略列表”中单击“新建”。依次选择或输入相应参数。单击“应用”。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	untrust *
目的安全区域	dmz *
源地址	请选择或输入IP地址 [多选]
目的地址	10.0.10.0/24 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

☑ IPS

IPS策略 protecthttp

Step 6 配置 IPS 策略保护内部网络 PC。

创建 IPS 策略 protectpc，在 IPS 策略中引入 default 策略模板。选择“UTM > 入侵防御 > 策略”。单击“新建”，指定策略的名称为 protectpc。在同步策略/策略模板中，选择“default”，单击“应用”。



应用 IPS 策略。 选择“防火墙 > 安全策略 > 转发策略”。 在“转发策略列表”中单击“新建”。依次选择或输入相应参数。单击“应用”。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	trust *
目的安全区域	untrust *
源地址	10.0.0.0/24 多选
目的地址	请选择或输入IP地址 多选
用户	请选择或输入用户或用户组 多选
服务	请选择服务 多选
时间段	all
动作	permit *
描述	

☑ IPS

IPS策略 protectpc

实验结果

实验结果：CLI 和 WEB

1. 当 Internet 上的恶意用户向内网 HTTP 服务器发起严重级别以上的 HTTP 攻击时，连接被阻断。
2. 当内网用户试图访问符合 default 模板中定义攻击特征的恶意网站时，连接被阻断。

12.3 UTM AV 防病毒实验

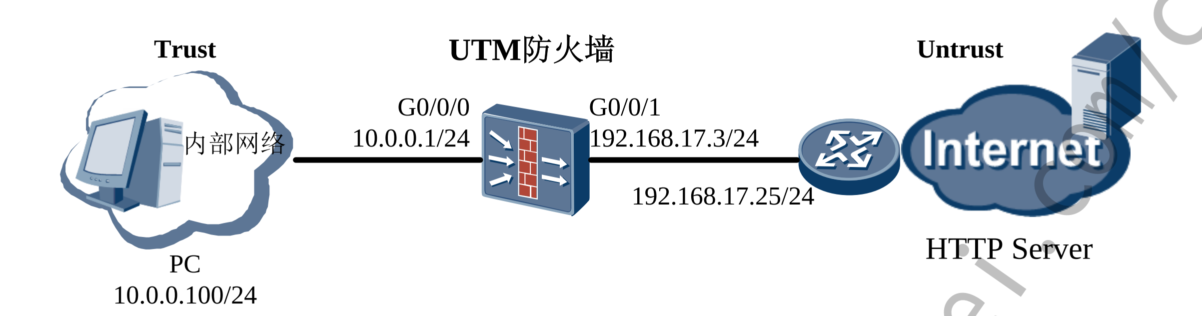
实验目的

使用（CLI）或（WEB）在 USG 上配置 AV 功能，保护企业内部用户访问 Internet 上的网页和 FTP 服务器时不受病毒感染。

组网设备

1. USG2000 或 USG5000 防火墙一台（V3R1 版本），PC 一台
2. 要求防火墙能够链接互联网

实验拓扑图



实验步骤 - CLI

Step 1 配置运行模式为 UTM 模式。

```
<USG> system-view
[USG] runmode utm
```

切换运行模式需要重启设备后才生效。请根据系统提示操作，推荐选择保存配置后重启。

Step 2 完成 USG 基本配置(略)。

需要注意，为使防火墙能够接入互联网，需要配置缺省路由，下一跳地址为 Internet 上与 USG 直接相连的路由器接口的 IP 地址。

```
[USG] ip route-static 0.0.0.0 0 192.168.17.254
```

Step 3 配置 AV 全局参数。

```
[USG] av enable
[USG] av scan-level 2
[USG] av max-decompress-layer 10
```

Step 4 创建 AV 策略并配置 AV 策略的公共部分。

```
[USG] av policy policy1
[USG-av-policy-policy1] description http and ftp server
[USG-av-policy-policy1] password-protected-file action permit
[USG-av-policy-policy1] deep-compressed-file action permit
[USG-av-policy-policy1] malformed-file action permit
[USG-av-policy-policy1] large-file action permit
```

Step 5 配置对 HTTP 协议文件的 AV 策略

```
[USG-av-policy-policy1] undo smtp enable
[USG-av-policy-policy1] undo pop3 enable
[USG-av-policy-policy1] http action block
[USG-av-policy-policy1] undo http upload enable
```

```
[USG-av-policy-policy1] http web-push-notification find-virus
[USG-av-policy-policy1] http scan-mode intelliscan
[USG-av-policy-policy1] http enable
[USG-av-policy-policy1] http max-file-size 10
[USG-av-policy-policy1] http download enable
[USG-av-policy-policy1] http resume-transfer enable
```

Step 6 配置对 FTP 协议文件的 AV 策略

```
[USG-av-policy-policy1] ftp action block
[USG-av-policy-policy1] ftp push-notification the file has security risks
[USG-av-policy-policy1] ftp scan-mode intelliscan
[USG-av-policy-policy1] ftp enable
[USG-av-policy-policy1] ftp max-file-size 10
[USG-av-policy-policy1] ftp upload enable
[USG-av-policy-policy1] ftp download enable
[USG-av-policy-policy1] ftp resume-transfer enable
[USG-av-policy-policy1] quit
```

Step 7 配置 Trust 和 Untrust 域间防火墙策略并应用 AV 策略，保护内网主机不受病毒侵害。

```
[USG] policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound] policy 5
[USG-policy-interzone-trust-untrust-outbound-5] action permit
[USG-policy-interzone-trust-untrust-outbound-5] policy source address-set internal
[USG-policy-interzone-trust-untrust-outbound-5] policy av policy1
```

实验步骤 – Web

Step 1 配置接口基本参数(略)。

Step 2 配置静态路由，保证网络连通，防火墙能够连接互联网。选择 "路由 > 静态 > 静态路由"。在"静态路由列表"中，单击"新建"，配置下一跳地址为：192.168.17.254，单击 "应用" 。



Step 3 配置运行模式为 UTM 模式。选择“UTM > 基本配置 > 基本配置”。 选中“启动”。 单击“应用”。 选择“保存配置并重启”或“直接重启”，单击“确定”。

推荐选择“保存配置并重启”，先保存配置再重启设备，否则设备重启后，未保存的配置信息将丢失。

UTM > 基本配置 > 基本配置

基本配置

UTM功能 ☑ 启用 应用

只有启用UTM功能并且有相应的License时，入侵防御、反病毒、URL过滤和垃圾邮件过滤功能才可以使用。

Step 4 配置 AV 全局参数。选择“UTM > 反病毒 > 策略”。 在“配置全局参数”区域框中配置全局参数。单击“应用”。

UTM > 反病毒 > 策略

配置全局参数

AV功能 ☑ 启用

扫描等级 中

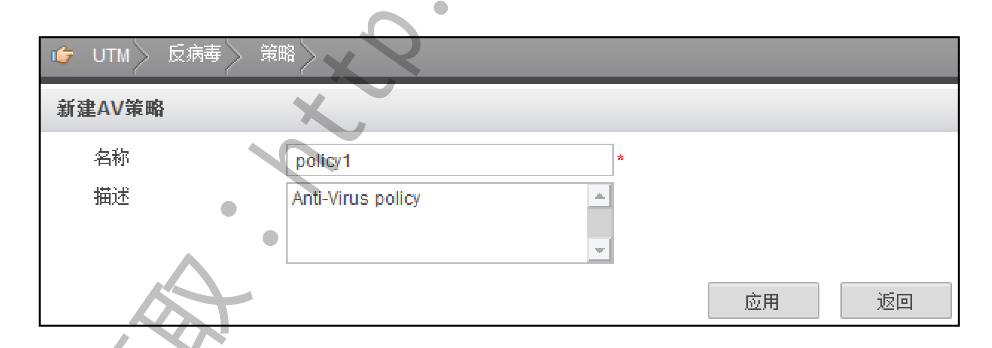
最大解压层数 10 <2-20>层

安全改善计划 ☐ 启用

参与安全改善计划后，设备可以在线收集您所在的网络的安全性问题，包括病毒以及攻击的信息，这些信息将发送给HuaweiSymantec安全服务中心，以帮助我们更好的保护您的网络。

应用

Step 5 配置 AV 策略。选择“UTM > 反病毒 > 策略”。 单击“新建”。 在“新建策略”界面配置名称 policy1。单击“应用”。



Step 6 在“HTTP 协议配置”区域框中配置各参数

HTTP协议配置

病毒扫描 启用
HTTP传输模式 上传 下载
断点续传 启用
传输体验 启用
文件大小上限 1 <1-20>MB
文件扫描方式 智能扫描 指定扩展名扫描 配置
响应方式 告警
推送内容

Step 7 在“FTP 协议配置”区域框中配置各参数。

1. 在“SMTP 协议配置”区域框中取消选中“病毒扫描”对应的复选框，关闭 SMTP 协议的病毒扫描开关。
2. 在“POP3 协议配置”区域框中取消选中“病毒扫描”对应的复选框，关闭 POP3 协议的病毒扫描开关。
3. 单击“应用”。



Step 8 应用 AV 策略。选择“防火墙 > 安全策略 > 转发策略”。 在“转发策略列表”中单击“新建”。依次选择或输入相应参数。单击“应用”。

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	trust *	
目的安全区域	untrust *	
源地址	10.0.0.0/24	多选
目的地址	请选择或输入IP地址	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

☐ IPS

☑ AV

AV策略 policy1

实验结果

实验结果：（CLI）和（WEB）

1. 当用户访问带病毒的 Web 页面时，阻断连接。
2. 当用户通过 FTP 上传和下载带病毒的文件时，阻断连接。

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- 1、**华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的 “华为账号” 和注册账号的 “email地址” 到 *Learning@huawei.com 申请权限。*
- 2、**华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入 “*华为培训->面授培训*” ，在具体课程页面即可下载教材。
- 3、**华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- 4、**学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform),* 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。**您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。** （http://support.huawei.com/ecommunity/bbs/list_2247.html ）

